

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2003年10月9日 (09.10.2003)

PCT

(10) 国際公開番号
WO 03/083646 A1

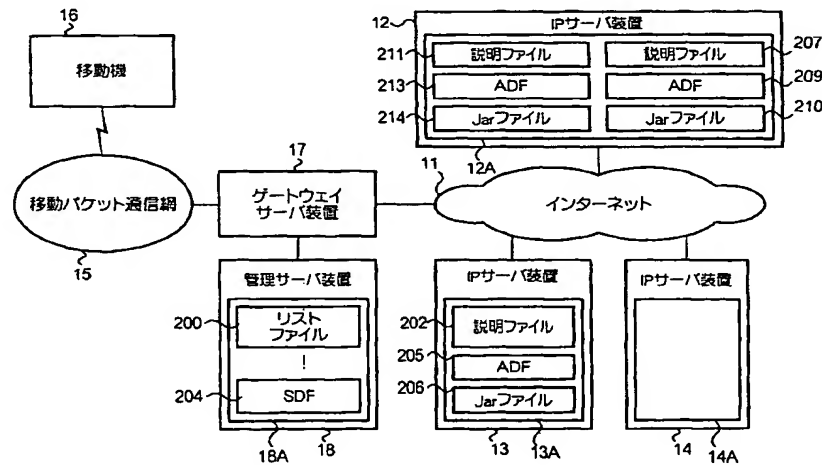
- (51) 国際特許分類⁷: G06F 9/06, 13/00, H04M 11/00
- (21) 国際出願番号: PCT/JP03/03974
- (22) 国際出願日: 2003年3月28日 (28.03.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2002-101756 2002年4月3日 (03.04.2002) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.)
[JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 Tokyo (JP).

- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 渡邊 信之 (WATANABE, Nobuyuki) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 澤田 久徳 (SAWADA, Hisanori) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 西尾 英昭 (NISHIO, Hideaki) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 中村 友則 (NAKAMURA, Tomonori) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 三浦 史光 (MIURA, Fumiaki) [JP/JP]; 〒100-6150 東京都千

[続葉有]

(54) Title: DISTRIBUTION METHOD, DISTRIBUTION SYSTEM, AND TERMINAL DEVICE

(54) 発明の名称: 配信方法、配信システム及び端末装置



16...MOBILE DEVICE
15...MOBILE PACKET COMMUNICATION NETWORK
17...GATEWAY SERVER DEVICE
18...MANAGEMENT SERVER DEVICE
200...LIST FILE
12...IP SERVER DEVICE
211...EXPLANATION FILE
207...EXPLANATION FILE

214...Jar FILE
210...Jar FILE
11...INTERNET
13...IP SERVER DEVICE
202...EXPLANATION FILE
206...Jar FILE
14...IP SERVER DEVICE

(57) Abstract: A mobile device (16) capable of starting Java-AP software acquires an ADF (205) from an IP server device (13). By using the ADF (205), the mobile device (16) receives an SDF (security description file) (204) from a management server device (18) managed by a reliable organization (communication company managing a mobile packet communication network (15)). Next, by using the ADF (205), the mobile device (16) acquires a Jar file (206) from an IP server device (13). The mobile device (16) installs in itself Java-AP software containing these files. The Java-AP realized by starting the Java-AP software operates within a range of authority represented by the policy information included in the SDF (204).

[続葉有]



代田区 永田町二丁目 1 1 番 1 号 山王パークタワー
株式会社エヌ・ティ・ティ・ドコモ 知的財産部内
Tokyo (JP). 富岡 淳樹 (TOMIOKA, Atsuki) [JP/JP]; 〒
100-6150 東京都 千代田区 永田町二丁目 1 1 番 1 号
山王パークタワー 株式会社エヌ・ティ・ティ・ド
コモ 知的財産部内 Tokyo (JP).

(74) 代理人: 川崎 研二 (KAWASAKI, Kenji); 〒103-0027 東
京都 中央区 日本橋一丁目 2 番 1 0 号 東洋ビルデ
ィング 7 階 朝日特許事務所 Tokyo (JP).

(81) 指定国 (国内): AU, BR, CA, CN, ID, IN, JP, KR, NO,
NZ, PH, PL, SG, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY,
CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC,
NL, PT, RO, SE, SI, SK, TR).

添付公開書類:

— 国際調査報告書

2 文字コード及び他の略語については、定期発行される
各 PCT ガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

(57) 要約: Java-AP ソフトウェアを起動することができる移動機 16 が、IP サーバ装置 13 から ADF 205 を
取得し、この ADF 205 を用いて信頼できる機関 (移動パケット通信網 15 を管理する通信事業者) が管理す
る管理サーバ装置 18 から SDF (セキュリティ記述ファイル) 204 を受信し、次いで、ADF 205 を用いて
IP サーバ装置 13 から Jar ファイル 206 を取得し、これらのファイルを内包する Java-AP ソフトウェ
アを自身にインストールする。この Java-AP ソフトウェアを起動することで実現される Java-AP は、
SDF 204 に内包されているポリシー情報で表される権限の範囲内で動作する。

明細書

5 配信方法、配信システム及び端末装置

技術分野

本発明は、端末装置にアプリケーションソフトウェアを配信する技術に関する。

10

背景技術

Java（登録商標）プログラミング言語に従って記述されたプログラムを実行してJava-AP（Javaアプリケーション）を実行する機能と、この種のプログラムを含むJava-APソフトウェアを、
15 ネットワークを介してダウンロードする機能とを備えた移動機が普及している。

Java-APソフトウェアとして、Jar（Java Archive）ファイルとADF（Application Descriptor File）とがある。ここで、Jarは、それが実行されることにより、あるJava-APをユーザに提
20 供するプログラムを内包している。また、ADFはJarファイルに依存しており、例えば、Jarファイルの格納位置を示すURL（以後、パッケージURL）、Jarファイルのサイズを示す情報、Jarファイルの最終変更日時を示す情報等を必須情報として内包している。

移動機は、次のような手順で、所望のJava-APに関連したソフトウェアのダウンロードを行う。まず、移動機は、WWW（World Wide
25 Web）を構成するサーバ装置から所望のJava-APに関連したADFを取得する。

ADFを取得した移動機はこのADFの内容を調べるとともに、その移動機に設けられたメモリの空き容量を調べ、所望のJava-APに

2

関連した J a r ファイルを当該移動機にインストール可能であるか否かを判断する。そして、インストール可能と判断すると、移動機は、A D F に含まれていたパッケージ URL を用いて、WWW を構成するサーバ装置から J a r ファイルを取得する。この J a r ファイルには、J a v a - A P ソフトウェアが格納されている。従って、この J a r ファイルの取得をもって J a v a - A P ソフトウェアのダウンロードは完了する。その後、移動機においては、ダウンロードされた J a v a - A P ソフトウェアのインストールが行われ、当該 J a v a - A P ソフトウェアは起動要求さえあれば実行される状態となる。

ところで、移動機内で実行される J a v a - A P の挙動についての制限は、通信アプリケーションなどの移動機が元から備えているネイティブアプリケーションの挙動についての制限よりも厳しくなっている。例えば、J a v a - A P は、移動機内の電話番号データなどの秘匿性の高い情報を参照することができないようになっている。このような厳しい制限を課すことにより、悪意をもって作成された J a v a - A P、あるいは不具合を有する J a v a - A P によって移動機内の秘密性の高い情報が漏洩したり改竄されたりする事態を確実に回避することができる。

しかし、上述した厳しい制限を全ての J a v a - A P に対して一律に課すだけでは、ユーザや I P（情報提供事業者）の希望を満たすことはできない。例えば、ある程度の信頼性が保証されるのであれば、J a v a - A P に移動機に格納された個人情報参照する権限を与えてもよいと感じるユーザがいると思われる。また、I P にも、移動機に格納されている個人情報や移動機が有する多数の機能を使用する、より魅力的な J a v a - A P を提供したいという希望がある。

これらの希望を満たすべく、移動機のユーザに対して通信サービスを提供する通信事業者等の信頼できる機関が J a v a - A P に権限を与え、この権限を移動機に通知し、当該権限に基づいて移動機が当該 J a v a - A P の挙動を制限するという仕組みが考えられる。この仕組みで

は、権限の信頼性を保証するために、信頼できる機関以外の他者が権限の付与・管理に関与し得ないようにすべきである。

J a v a - A P ソフトウェアのダウンロード手順に上述の仕組みを適用する場合、信頼できる機関が A D F あるいは J a r ファイルに権限を示す情報を内包させるのが妥当である。ここで、J a r ファイルは I P により随時更新されるので、I P が保有するのが適当である。しかし、I P が J a r ファイルを保有するとすると、信頼できる機関は J a r ファイルを保有し得ない。従って、信頼できる機関は、このような J a r ファイルよりは、むしろ A D F を保有し、この A D F に権限を示す情報を内包させるのが妥当であるといえることができる。

しかし、A D F は J a r ファイルに依存した内容となることから、I P が手元の J a r ファイルを更新すると、信頼できる機関が保有している A D F の更新も必要になってくる。ここで、信頼できる機関は、他社の関与を排するように A D F を管理することが必要であるから、信頼できる機関と I P が連携して A D F を更新することとなり、その作業が複雑なものになることが懸念される。また、J a r ファイルを更新せずとも、A D F の更新が必要となることがある。例えば、I P において、ある J a r ファイルへのアクセスが殺到し、この J a r ファイルを他のサーバ装置へ移動する場合である。この場合、J a r ファイルの格納位置が変更されるから、A D F に内包されているパッケージ URL を変更する必要がある。しかしながら、A D F は信頼できる機関において他者の関与を排するように管理されるのであるから、A D F の更新作業は複雑な作業となると予想される。

25 発明の開示

本発明は、上述した事情に鑑みて為されたものであり、権限に応じた挙動をアプリケーションに許可する端末装置に対し、依存関係にある複数のファイルを配信することによってそのアプリケーションを実現するためのソフトウェアを配信可能な仕組みを提供することを目的として

いる。

上述した課題を解決するために、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有した配信システムが、前記アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信する過程と、前記端末装置が、前記配信システムから送信されてくるアプリケーション記述ファイルに内包されている前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する過程と、前記配信システムが、前記通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で前記端末装置に送信する過程と、前記端末装置が、前記配信システムから送信された前記アプリケーション記述ファイルに内包されている前記実体ファイルの格納位置を前記配信システムに通知する過程と、前記配信システムが、前記通知された実体ファイルの格納位置に基づいて、当該実体ファイルを前記端末装置に送信する過程とを有する配信方法を提供する。

この方法によれば、配信システムが、アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信し、端末装置が、得たアプリケーション記述ファイルに内包されているセキュリティ記述ファイルの格納位置を配信システムに通知し、配信システムが、通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で端末装置に送信し、端末装

5

置が、配信システムから送信されてくるアプリケーション記述ファイルに内包されている実体ファイルの格納位置を前記配信システムに通知し、配信システムが、通知された実体ファイルの格納位置に基づいて、当該実体ファイルを端末装置に送信する。

- 5 また、本発明は、ネットワーク内の装置との通信を行うための通信部と、記憶部と、制御部とを具備し、前記制御部は、(a) アプリケーションを実現するためのソフトウェアを内包した実体ファイルの格納位置と、前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルの格納位置を示す情報を含んだ第1の配信要求を前記通信部により前記ネットワーク内の配信システムに送信することにより、前記配信システムにおける情報提供サーバ装置に格納されたアプリケーション記述ファイルを前記配信システムから前記通信部により受信し、前記記憶部に格納する手段と、(b) 前記配信システムから受信されたアプリケーション記述ファイルに内包されている前記セキュリティ記述ファイルの格納位置を示す情報を含んだ第2の配信要求を前記通信部により前記配信システムに送信することにより、前記配信システムにおける管理サーバ装置に記憶されたセキュリティ記述ファイルを前記配信システムから前記通信部により受信し、前記記憶部に格納する手段と、(c) 前記配信システムから受信されたアプリケーション記述ファイルに内包されている実体ファイルの格納位置を示す情報を含む第3の配信要求を前記通信部により前記配信システムに送信することにより、前記配信システムにおける情報提供サーバに格納された実体ファイルを前記配信システムから前記通信部により受信し、前記記憶部に格納する手段と、
- 10 (d) 前記記憶部に記憶された実体ファイルに含まれるソフトウェアの実行が指示された場合に、前記記憶部に記憶された該実体ファイルに対応したセキュリティ記述ファイルに含まれる権限情報に従い、該ソフトウェアの実行により実現されるアプリケーションの挙動を制限する手
- 15
- 20
- 25

6

段とを有する端末装置を提供する。

この場合において、前記配信システムは、前記セキュリティ記述ファイルを暗号化して前記端末装置に送信することによってセキュリティを確保しており、前記端末装置の制御部は、前記配信システムによって
5 送信されてくる暗号化されたセキュリティ記述ファイルを復号化する手段を具備していてもよい。

また、前記端末装置の制御部は、前記通信部により、セキュリティの確保された通信路を介して前記セキュリティ記述ファイルを受信してもよい。

10 この場合において、前記端末装置の制御部は、暗号化通信により前記セキュリティ記述ファイルを受信してもよい。

また、前記端末装置の制御部は、前記通信部により、移動通信網および専用線を介して前記セキュリティ記述ファイルを受信してもよい。

15 この場合において、前記端末装置の制御部は、移動通信網を介した暗号化通信により前記セキュリティ記述ファイルを受信してもよい。

好ましい態様において、前記端末装置の制御部におけるアプリケーションの挙動を制限する手段は、前記セキュリティ記述ファイルに内包された権限情報に基づき、資源の利用を制限してもよい。

20 この場合において、前記資源は前記端末装置内部のハードウェア資源であってもよいし、前記端末装置外部の、当該端末装置が使用可能なハードウェア資源であってもよいし、前記端末装置内部のソフトウェア資源であってもよいし、前記端末装置外部の、当該端末装置が使用可能なソフトウェア資源であってもよいし、前記端末装置が使用可能なネットワーク資源であってもよい。

25 好ましい態様において、前記端末装置の制御部におけるアプリケーションの挙動を制限する手段は、前記権限情報に基づき資源の利用の種類を判断してもよい。

好ましい態様において、前記アプリケーション記述ファイルは前記端末装置に通信サービスを提供する通信事業者の公開鍵を内包し、前記セ

セキュリティ記述ファイルは前記通信事業者の秘密鍵で署名されており、前記制御部は、前記配信システムによって送信されてくるセキュリティ記述ファイルの正当性を前記アプリケーション記述ファイルに内包されている公開鍵を用いて検証し、その正当性が検証された場合にのみ、
5 前記配信システムに対し前記実体ファイルの格納位置を通知する端末装置を提供する。

また、好ましい態様において、前記アプリケーション記述ファイル及び前記セキュリティ記述ファイルは、対応するアプリケーションに割り当てられたアプリケーション識別子を内包しており、前記制御部は、前
10 記配信システムによって送信されてくるアプリケーション記述ファイルに内包されたアプリケーション識別子と、前記配信システムによって送信されてくるセキュリティ記述ファイルに内包されたアプリケーション識別子とを比較し、両者が一致した場合にのみ、前記配信システムに前記実体ファイルの格納位置を通知する端末装置を提供する。

また、前記アプリケーション記述ファイルに記述された前記セキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ、前
15 記端末装置の制御部は、前記セキュリティ記述ファイルの格納位置を前記配信システムに通知するようにしてもよい。

好ましい態様において、前記セキュリティ記述ファイルは、対応する
20 アプリケーションの有効期限を示す期限情報を内包しており、前記端末装置の制御部は、前記配信システムに対して前記セキュリティ記述ファイルの格納位置を時系列的に繰り返し通知することによって、前記配信システムから当該セキュリティ記述ファイルが時系列的に繰り返し受信し、繰り返し受信される前記セキュリティ記述ファイルに内包されて
25 いる前記期限情報に基づいて、前記アプリケーションの有効期限を更新する手段を具備していてもよい。

この場合、前記端末装置は、前記配信システムから前記セキュリティ記述ファイルが正当に配信されてきた場合にのみ、前記アプリケーションの有効期限を更新するようにしてもよい。

好ましい態様において、前記端末装置は移動機であってもよい。

また、本発明はアプリケーションを実現するためのソフトウェアを内包した実体ファイルと、前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルと、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した1または複数のサーバ装置とを有し、前記1または複数のサーバ装置のうち前記セキュリティ記述ファイルを格納するサーバ装置は、セキュリティ記述ファイルを管理する権限の与えられた管理サーバ装置であり、各々の前記サーバ装置は、ファイルの格納位置が通知されると当該ファイルをその通知元に返送する手段を有し、前記管理サーバ装置は、前記セキュリティ記述ファイルの格納位置が通知されると当該セキュリティ記述ファイルをセキュリティが確保された状態で通知元に返送する配信システムを提供する。

図面の簡単な説明

図1は本発明の実施の一形態に係る配信システムの構成を示すブロック図である。

図2は同システムに特有のADFのデータ構成を示す概念図である。

図3は同システムにおいて管理サーバ装置に格納されているSDFのデータ構成を示す概念図である。

図4は同SDFに内包されるポリシー情報の内容を示す概念図である。

図5は同システムを構成する移動機の構成を示すブロック図である。

図6は同移動機の機能構成を示す概念図である。

図7は同移動機がJava-APソフトウェアをダウンロードしインストールする処理の流れを示すフローチャートである。

図8は同移動機がJava-APソフトウェアの有効期限を更新す

る処理の流れを示すフローチャートである。

図 9 は同配信システムの動作を説明するためのブロック図である。

図 10 は同配信システムにて配信されるリストページを示す図である。

5 図 11 は同配信システムを構成する I P サーバ装置が格納している説明ファイルの内容を示す図である。

図 12 は同配信システムにて配信される説明ページを示す図である。

図 13 は同 I P サーバ装置が格納している説明ファイルの内容を示す図である。

10 図 14 は同配信システムにて配信される説明ページを示す図である。

図 15 は同配信システムを構成する I P サーバ装置 13 が格納している説明ファイルの内容を示す図である。

図 16 は同配信システムにて配信される説明ページを示す図である。

15 図 17 は同配信システムの動作を説明するためのシーケンス図である。

図 18 は同配信システムの動作を説明するためのシーケンス図である。

図 19 は同配信システムの動作を説明するためのシーケンス図である。

20 図 20 は同配信システムの動作を説明するためのシーケンス図である。

図 21 は移動機にて表示される画面を示す図である。

図 22 は同配信システムの他の動作を説明するためのブロック図である。

25 図 23 は同配信システムの他の動作を説明するためのシーケンス図である。

図 24 は、S D F の有効性を問い合わせるための処理を行う移動機の制御部内の構成を示す図である。

図 25 は、S D F の有効性の問い合わせの動作を示すタイムチャート

である。

発明を実施するための最良の形態

以下、図面を参照して、本発明の実施の一形態である配信システムについて説明する。なお、図面において、共通する部分には同一の符号が付されている。

(1) 構成

図 1 に示されるように、この配信システムにおいて、IPサーバ装置 12～14 は、インターネット 11 に接続されている。IPサーバ装置 12 は第 1 の IP (Internet Provider) によって管理されており、IPサーバ装置 13 および 14 は第 1 の IP と異なる第 2 の IP により管理されている。そして、IPサーバ装置 12～14 は WWW を構成しており、それぞれ一般的な WWW サーバ装置と同様のハードウェアおよび機能を有する。移動パケット通信網 15 は、通信事業者が移動パケット通信サービスを提供するために用いる網である。移動機 16 は、この移動パケット通信網 15 との間で無線パケット通信を行うことが可能である。ゲートウェイサーバ装置 17 は、移動パケット通信網 15 と同じ通信事業者により管理されている。このゲートウェイサーバ装置 17 は、移動パケット通信網 15 とインターネット 11 とを接続する装置であり、一般的なゲートウェイサーバ装置の構成と同様の構成を有する。管理サーバ装置 18 は、専用線によりゲートウェイサーバ装置 17 に接続されている。この管理サーバ装置 18 もまた WWW を構成し、一般的な WWW サーバ装置と同様のハードウェアおよび機能を有する。ゲートウェイサーバ装置 17 は、移動パケット通信網 15 とインターネット 11 との間のパケット中継、管理サーバ装置 18 と移動パケット通信網 15 との間のパケット中継および管理サーバ装置 18 とインターネット 11 との間のパケット中継を行う。移動機 16 は、この中継機能を利用することにより、移動パケット通信網 15 およびインターネット 11 を介して IP サーバ装置 12～14 とパケット通信を行うことが可能で

ある。なお、実際の配信システムには多数の移動機が存在するが、図面が繁雑になるのを避けるために一つの移動機 16 のみが図示されている。これと同様の理由により、3つのIPサーバ装置 12～14 のみが図示されている。

- 5 この配信システムにおいて、移動機 16 は、インターネット 11 上の所望のサイトから Java-AP ソフトウェアを受け取ることができる。この移動機 16 が受け取ることができるソフトウェアは、トラステッド Java-AP に関するものと、非トラステッド Java-AP に関するものに大別される。ここで、トラステッド Java-AP ソフト
- 10 ウェアは、移動パケット通信網 15 を管理する通信事業者が、IPサーバ装置 12～14 を管理する IP との契約に基づいて信頼性を保証した Java-AP ソフトウェアである。また、非トラステッド Java-AP ソフトウェアは、トラステッド Java-AP ソフトウェア以外の Java-AP ソフトウェアである。
- 15 管理サーバ装置 18 は、この配信システム内を流通する各トラステッド Java-AP ソフトウェアについて SDF（セキュリティ記述ファイル）を各々記憶している。この SDF は、移動パケット通信網 15 を管理する通信事業者によって作成されるファイルであり、移動機のトラ
- 20 ステッド API（Application Interface）を使用する Java-AP ソフトウェアを移動機にダウンロードする際に必須のファイルである。なお、トラステッド API については後述する。図 3 に示されるように、SDF は、トラステッド Java-AP ソフトウェアを識別するための APID、ポリシー情報、および有効期限を有する。これらの情報は通
- 25 信事業者の秘密鍵を用いて暗号化されている。ここで、ポリシー情報は、トラステッド Java-AP の移動機 16 内での挙動に対する制限を示す情報である。なお、このポリシー情報およびこれに基づいて行われる Java-AP の挙動の制限の詳細については後述する。

本実施形態では、移動機 16 から所望のトラステッド Java-AP ソフトウェアの配信要求が送信された場合に、IPサーバ装置 12～1

4の1つから移動機16にそのトラステッドJava-APソフトウェアにおけるADFが配信される。ここで、トラステッドJava-APソフトウェアのADFには、Jarファイルの所在を示すURLの他、このトラステッドJava-APソフトウェアに対応したSDFの所在を示すURLと、そのSDFの暗号化に用いられた秘密鍵と対をなす公開鍵が含まれている。このADFを受信した移動機16は、ADF内のURLを用いてSDFを取得し、ADF内の公開鍵を用いてSDFを復号化する。そして、最後に移動機16は、ADFに含まれているJarファイルのURLを用いて、Jarファイルを取得する。その後、移動機16において、トラステッドJava-APソフトウェアが実行されるときには、SDFに基づいて、トラステッドJava-APの挙動の制限が行われる。これが本実施形態の特徴の1つである。図1に示すとおり、SDFの送信は移動パケット通信網15を通して行われ、管理サーバ装置18とゲートウェイサーバ装置17は専用線によって接続されている。

以下、この特徴との関連において、配信システムの各要素の構成を説明する。

IPサーバ装置12、13及び14は不揮発性メモリ12A、13A及び14Aをそれぞれ有する。

不揮発性メモリ12A、13Aおよび14Aは、ハードディスク等の不揮発性メモリであり、JarファイルおよびADFからなるJava-APソフトウェアと、Java-APソフトウェアの内容を移動機のユーザに説明するための説明ファイルとを記憶している。

不揮発性メモリ12A、13Aおよび14Aに記憶されている個々のJava-APソフトウェアは、トラステッドJava-APソフトウェアであるかも知れないし、非トラステッドJava-APソフトウェアであるかも知れない。トラステッドJava-APであるか非トラステッドJava-APであるかに拘わらず、全てのJava-APソフトウェアのADFには、WWWにおけるJarファイルの記憶位置を示

13

すパッケージURLや、Jarファイルのサイズを示す情報、Jarファイルの最終変更日時を示す情報等が記述されている。これらはJava-APソフトウェアのADFに記述されるべき項目として一般的に知られているものである。そして、トラステッドJava-APソフトウェアのADFは、これらの一般的に知られた情報の他に、図2に示されるように、そのトラステッドJava-APソフトウェアのAPIDと、Jarファイルのハッシュ値と、SDFがWWWにおいて記憶されている位置を示すURL（以下、SDF-URLと呼ぶ）と、そのSDFの暗号化に使用された秘密鍵と対をなす公開鍵とを内包している。ここで、公開鍵は、図示せぬCA（認証局）によって正当性が証明された通信事業者に対し、証明書として発行されるものである。

また、説明ファイルは、HTMLに従って記述されたテキストファイルである。移動機は、あるJava-APソフトウェアをダウンロードする場合に、それに先だって、このJava-APソフトウェアに対応した説明ファイルをダウンロードする必要がある。説明ファイルには、Java-APソフトウェアのダウンロードの指示をユーザから受け取るUI（ユーザインターフェイス）を構成するための情報が含まれている。移動機16は、この情報に従い、UI画面を表示する。ユーザは、このUI画面中の所望のJava-APを表すオブジェクトを指定する操作を移動機16に対して行うことができる。説明ファイルには、このようにしてユーザによって指定されるオブジェクトを、ダウンロード対象であるJava-APソフトウェアに対応するADFのWWWにおける所在を示すURLに対応付けるように記述されている。

IPサーバ装置12～14の各々は、以上説明した各ファイルをIPの指示に従って作成および更新する機能を備えている。

管理サーバ装置18は、ハードディスク等の不揮発性メモリ18Aを有する。管理サーバ装置18は、TCPコネクションを通信相手との間に確立する。管理サーバ装置18は、このTCPコネクションを介して、HTTPのGETメソッドを用いた要求メッセージを通信相手から受

信すると、当該GETメソッドに指定されたURLで特定されるファイルを不揮発性メモリ18Aから読み出し、このファイルを含むHTTPの応答メッセージを返送して当該コネクションを切断する。

また、上記不揮発性メモリ18Aには、ダウンロード可能なJava-APソフトウェアを移動機16のユーザに紹介するためのリストファイル200と、このリストファイル200に挙げられた各Java-APソフトウェアに各々対応したSDFとが記憶される。

これらのうちSDFは、既に図3を参照して説明した通りである。

リストファイル200は、HTMLに従って記述されたテキストファイルである。既に説明したように、移動機は、あるJava-APソフトウェアをダウンロードする場合に、それに関連した説明ファイルを取得する必要がある。既に説明したように、移動機16は、この説明ファイルを格納しているIPサーバ装置にアクセスするという方法により、この説明ファイルを取得することができる。しかし、このような直接的な方法以外に、本実施形態において移動機16は、次のような手順により所望のJava-APソフトウェアの説明ファイルを取得することもできる。まず、移動機16は、管理サーバ装置18にアクセスして、このリストファイル200を取得し、これに従い、UI画面を表示する。ユーザは、このUI画面中の所望のJava-APを表すオブジェクトを指定する操作を移動機16に対して行うことができる。リストファイル200は、このようにしてユーザによって指定されるオブジェクトを、ダウンロード対象であるJava-APソフトウェアの説明ファイルのWWWにおける所在を示すURLに対応付ける。移動機16は、このようにリストファイル200を介して得られるURLを用いて、IPサーバ装置から説明ファイルを取得するのである。

移動機16は、図5に示されるように、OS（オペレーティングシステム）ソフトウェア、Java-APを実行する環境を構築するためのJava-AP環境ソフトウェアおよび各種ネイティブAPソフトウェア等を記憶したROM16Aと、ROM16Aに接続されROM16

Aからプログラムを読み出して実行するCPU16Bと、CPU16Bに接続された表示部16Cと、不揮発性メモリ16Dと、RAM16Eと、通信部16Fと、操作部16Gとを有する。

- 表示部16Cは、例えば液晶表示パネルを有し、CPU16Bから供給されるデータを画像として表示する。不揮発性メモリ16Dは例えばSRAMやEEPROMであり、CPU16Bによりデータを読み書きされる。不揮発性メモリ16Dは、WWWを構成するサーバ装置（以後、Webサーバ装置）からダウンロードしたJava-APソフトウェアを記憶するために使用される。既に述べたように、本実施形態において、
- 「Java-APソフトウェア」という語は、「トラステッドJava-APソフトウェア」および「非トラステッドJava-APソフトウェア」の両方を指すのに用いられている。しかし、ある文脈において「Java-APソフトウェア」という語が「トラステッドJava-APソフトウェア」を指している場合もある。そのような文脈において、この語は、ADF、SDFおよびJarを含む概念と解釈されるべきである。また、ある文脈において、「Java-APソフトウェア」という語が「非トラステッドJava-APソフトウェア」を指している場合もある。そのような文脈において、この語はADFおよびJarを含む概念と解釈されるべきである。
- 通信部16Fは、移動パケット通信網15と無線パケット通信を行うものであり、CPU16Bと移動パケット通信網15との間でパケットを中継する。また、通信部16Fは、アンテナや無線送受信部の他に、通話のためのCODECやマイク、スピーカ等を備えている。従って、移動機16は、この通信部16Fにより、図示せぬ移動通信網を介して回線交換による通話を行うこともできる。操作部16Gは操作子を備え、操作子の操作に応じた信号をCPU16Bへ供給する。計時部16Hは、現在の年月日および時刻（以下、単に現在日時という）を計時する。なお、計時部16Hがより正確な現在日時を計時するために、例えば移動パケット通信網15の図示せぬ基地局から制御チャネルを介して定期

的に通知される現在日時に同期させるような処理を行ってもよい。

CPU 16 Bは、ROM 16 Aに記憶された各種プログラムに従って移動機 16 全体の制御を行う装置である。図示せぬ電源が投入されると、このCPU 16 BはRAM 16 Eをワークエリアとし、ROM 16 Aから図 6 のOSを読み出して実行する。CPU 16 Bは、このOSに従ってUI等を機能を提供する。OSは操作部 16 Gから供給される信号とUIの状態とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。

ユーザの指示がネイティブAPソフトウェアである通信ソフトウェアの起動を要求するものであれば、OSは通信ソフトウェアを起動して移動機 16 内にて通信APを実行する。この通信APを用いることで、ユーザは通話相手と通話をすることができる。

ユーザの指示がネイティブAPソフトウェアである電話帳APの起動を要求するものであれば、OSは電話帳ソフトウェアを起動して移動機 16 内にて電話帳APを実行する。この電話帳APを用いることで、ユーザは、不揮発性メモリ 16 Dに記憶された電話帳の内容（以後、電話帳データ）を参照・使用・変更することができる。

ユーザの指示がネイティブAPソフトウェアであるWebブラウザソフトウェアの起動を要求するものであれば、OSはWebブラウザソフトウェアを起動して移動機 16 内にてWebブラウザを実行する。このWebブラウザはUIを提供する。そして、Webブラウザは、ユーザから操作部 16 Gの操作により指示があると、UIの状態と操作部 16 Gから供給される信号とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。例えば、当該指示が指定されたファイルをWWWから取得する旨の場合には、通信部 16 Fを制御して当該ファイルを記憶したWebサーバ装置との間にTCPコネクションを確立し、このコネクションを介して、指定された位置を示すURLをGETメソッドに用いたHTTPの要求メッセージを送信し、この要求メッセージに対応する応答メッセージを受信し、当該コネクションを切断する。さらに、

Webブラウザは、受信した応答メッセージに内包されているファイルをHTMLに従って解釈し、Webページを内包するUIを生成し、ユーザに提供する。また、ユーザの指示がJava-APソフトウェアのダウンロードを要求するものである場合には、Webブラウザは、この

5 指示を次に述べるJAM (Java Application Manager) に通知する。具体的には、Webページにおいて、クリック操作またはプレス操作により、オブジェクトタグが指定されているアンカータグで表されるアンカーが指定されると、Webブラウザは当該オブジェクトタグのdata属性に指定されているURLを抽出し、当該URLからのJava-APソフトウェアのダウンロードが要求されたことをJAMに通知する。

10 ユーザの指示がネイティブAPソフトウェアであるJAMソフトウェアの起動を要求するものであれば、OSはJAMソフトウェアを起動して移動機16内にてJAMを実行する。JAMは、移動機16にインストールされているJava-APソフトウェアの一覧をユーザに提示し、ユーザにより指定されたJava-APソフトウェアを起動する。

15 具体的には、JAMに対するユーザの指示がJava-APソフトウェアの起動を要求するものであれば、Java-AP環境ソフトウェアが起動されて移動機16内にJava-AP環境が実行される。そして、指定されたJava-APソフトウェアが起動されてJava-AP環境内にJava-APが実行される。Java-AP環境は、携帯端末に適した軽量のJava仮想マシンであるKVMと、Java-APに対して提供されるAPIとを有する。Java-APに対して提供されるAPIは、通信事業者がIPとの契約に基づいて信頼性を保証したJava-AP（以後、トラステッドAP）のみに使用が許可されるトラステッドAPIと、あらゆるJava-APに使用が許可される非トラステッドAPIとに分けられる。

20 25

(2) 動作

以下、本実施形態の動作を説明する。

(2-1) 移動機16によるJava-APソフトウェアのダウンロー

ド

JAMは、Java-APのダウンロードを要求する指示がWebブラウザから通知されると、Java-APソフトウェアを移動機16にダウンロードしインストールする処理を行う。この処理の流れを図7に示す。なお、図7では、移動機16が説明ファイルを取得するまでの過程は省略されている。説明ファイルの取得までの過程は、幾つかの態様があるので、後に具体的な動作例を挙げて説明する。図7に示されるように、JAMは、まず、Java-APソフトウェアのダウンロードを要求する指示があったか否かを判定する（ステップS11）。そして、Java-APソフトウェアのダウンロードを要求する指示がWebブラウザから通知されると、そのJava-APソフトウェアに対応するADFをIPサーバ装置12～14のいずれかから取得する（ステップS12）。具体的には、JAMは、IPサーバ装置12～14のうちADFを格納しているものとの間にTCPコネクションを確立し、ADFの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信してADFを取得した後、このTCPコネクションを切断する。そして、JAMは、応答メッセージに内包されているADFを不揮発性メモリ16Dに書き込む。

次いで、JAMは、ダウンロードしようとしているJava-APソフトウェアを移動機16にインストール可能か否かをADFの内容に基づいて判定する（ステップS13）。ここでは、ADFに記述されていたJarファイルのサイズと、不揮発性メモリ16D内のJarファイルを記憶可能な空き容量とを比較する等の、従来と同様の基準に従って判定すればよい。

ここで、インストール可能と判定された場合には（ステップS13；Yes）、JAMは、ダウンロードしようとするJava-APソフトウェアがトラステッドJava-APソフトウェアであるか否かを判定する（ステップS14）。具体的には、JAMは、ステップS12において取得したADF内にSDF-URLが記述されているか否かを

確認し、記述されていれば、このJ a v a - a p ソフトウェアに対応するS D Fが存在する、即ち、トラステッドJ a v a - A P ソフトウェアであると判定するし、その記述がなければ非トラステッドJ a v a - A P ソフトウェアであると判定する。

- 5 そして、ダウンロードしようとするJ a v a - A P ソフトウェアが非トラステッドJ a v a - A P ソフトウェアであると判定された場合には（ステップS 1 4 ; N o）、従来と同様のダウンロードおよびインストール処理が行われる（ステップS 1 5）。

- 10 一方、ダウンロードしようとするJ a v a - A P ソフトウェアがトラステッドJ a v a - A P ソフトウェアと判定された場合には（ステップS 1 4 ; Y e s）、J A Mは、このソフトウェアに対応するS D Fを管理サーバ装置1 8から取得する（ステップS 1 6）。すなわち、J A Mは、管理サーバ装置1 8との間にT C Pコネクションを確立し、このコネクションを介して、A D F内に記述されているS D F - U R Lで示される位置に記憶されたS D Fの送信を管理サーバ装置1 8に要求する
15 内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信してS D Fを取得した後、上記コネクションを切断する。

- 20 前述したように、トラステッドJ a v a - A P ソフトウェアに対応するS D Fは、A P I Dとポリシー情報と有効期限とを内包し、さらに通信事業者の秘密鍵により署名（暗号化）されている。そこで、J A Mは、応答メッセージに内包されているS D Fの署名を、既を取得しているA D Fから抽出された公開鍵を用いて検証し（復号し）、このS D Fの正当性を判断する（ステップS 1 7）。正当性が確認された場合（ステップS 1 7 ; Y e s）、J A Mは、S D Fを不揮発性メモリ1 6 Dに書き
25 込む。

次いで、J A Mは、S D Fに内包されているA P I Dと、既を取得しているA D Fに内包されていたA P I Dとを比較し、両者が一致する可否かを判定する（ステップS 1 8）。

両者が一致すると判定された場合には（ステップS 1 8 ; Y e s）、

JAMは、Jarファイルを取得する（ステップS19）。具体的には、JAMは、ADFに内包されているパッケージURLで特定されるJarファイルを記憶したIPサーバ装置12～14のいずれかとの間にTCPコネクションを確立し、このJarファイルの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信してJarファイルを取得し、このTCPコネクションを切断する。

次に、JAMは、取得したJarファイルに対するハッシュ値を算出する（ステップS20）。ハッシュ値の算出に使用するハッシュ関数は任意であるが、移動機16で使用するハッシュ関数とADFに含まれるハッシュ値の算出時に使用されるハッシュ関数とは一致していなければならない。実際には、移動機16で使用するハッシュ関数を用いて、トラステッドJava-APソフトウェアを提供するIPがハッシュ値を算出してADFを生成することになる。

JAMは、算出したハッシュ値とADFから抽出したハッシュ値とを比較し、両者が一致した場合には（ステップS21；Yes）、取得したJarファイルを不揮発性メモリ16Dに書き込み、トラステッドJava-APソフトウェアのインストールに係る各種処理を行い（ステップS22）、インストールに成功した旨をユーザに通知する（ステップS23）。

以降、JAMは、トラステッドJava-APソフトウェアを実行するに際し、トラステッドJava-APの挙動を監視し、トラステッドAPIの使用を制限するが、この制限は不揮発性メモリ16Dに記憶されるSDF内のポリシー情報に従って行われることとなる。

なお、Java-APソフトウェアをインストール不可能と判断された場合（ステップS13；No）、SDFが正当でないと判断した場合（ステップS17；No）、SDFが有するAPIIDとADFが有するAPIIDが不一致の場合（ステップS18；No）、算出したハッシュ値とADFが有するハッシュ値とが不一致の場合（ステップS21；N

o) には、JAMは、インストールに失敗した旨をユーザに通知するとともに、移動機16の状態をステップS11以前の状態に戻す。

(2-2) 移動機16によるSDFの更新

- 5 トラステッドJava-APソフトウェアは、対応するSDFに内包されていた有効期限が経過するまでは移動機16によって実行可能である。この有効期限を更新する場合には、移動機16は、管理サーバ18から新たにSDFを取得する必要がある。そこで、以下では、JAMが、SDF内の有効期限が到来する度にその有効期限を更新する場合の
- 10 処理について、図8に示すフローを参照しながら説明する。

- 図8に示されるように、JAMは、移動機16内の計時部16Hによって計時される現在日時と、今までに取得した全てのSDFからそれぞれ抽出して不揮発性メモリ16Dに記憶した複数の有効期限とを常時監視しており、有効期限が到来したか否かを判断している（ステップS
- 15 31）。

- いずれか1つでも有効期限が到来すると（ステップS31; Yes）、JAMは、有効期限が到来したJava-APソフトウェアの名称とともに、有効期限が到来したので更新するか否かをユーザに問い合わせるメッセージを表示部16Cに表示してユーザの操作があるまで待機する。
- 20

- ユーザが有効期限を更新することを指示する操作を行うと、JAMはこの指示内容を解釈し（ステップS32; Yes）、この有効期限を更新すべきJava-APソフトウェアに対応するSDFを管理サーバ装置18から取得する（ステップS33）。具体的には、JAMは、不
- 25 揮発性メモリ16Dの記憶内容を参照し、有効期限を更新すべきJava-APソフトウェアのAPIDを内包したADFに内包されているSDF-URLを抽出し、このSDF-URLで示される位置に記憶されたSDFの送信を管理サーバ装置18に要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し

てSDFを取得した後、上記コネクションを切断する。

次いで、JAMは、上記SDF-URLを用いてSDFを取得できたか否かを判断する（ステップS34）。ここで、SDFを取得できない場合とは、何らかの事情でJava-APソフトウェアの使用を中断或いは中止させたいという理由から、通信事業者が、管理サーバ装置18
5 において上記のSDF-URLによって示される位置にSDFを記憶させていないことを意味している。その事情とは、例えば、IPの都合によってJava-APソフトウェアの使用を中止或いは中断させたい場合（例えば、ユーザが一定期間だけ試用できるソフトウェアを配信
10 するような場合）や、IPと通信事業者との間で締結されていた契約が失効した場合等である。

さて、JAMは、SDFの取得に成功すると（ステップS34；Yes）、SDFの署名を、既を取得しているADFに内包されている公開鍵を用いて検証し（復号し）、このSDFの正当性を判断する（ステップS35）。
15

正当性が確認されると（ステップS35；Yes）、JAMは、SDFに内包されているAPIDと、既を取得済みのADFに内包されているAPIDとを比較し、両者が一致するか否かを判定する（ステップS36）。両者が一致すると判定された場合には（ステップS36；Yes）、JAMは、取得したSDFを不揮発性メモリ16Dに既
20 書き込まれている以前のSDFに上書きし、これにより有効期限を更新する。

なお、ユーザの操作により有効期限を更新しないと判断された場合（ステップS32；No）、SDFを取得できなかった場合（ステップS34；No）、SDFが正当でないと判断した場合（ステップS35；No）、SDFが有するAPIDとADFが有するAPIDが不一致の場合（ステップS36；No）、JAMは、有効期限を更新しない旨をユーザに通知するとともに、移動機16の状態をステップS31以前の
25 状態に戻す。

（3）具体的動作

次に、上述したシステムの動作例について説明する。

なお、以下に述べる動作において、TCPコネクションの確立および切断動作についてはHTTPにおける一般的な動作となることから、それらの説明を省略する。また、前述のOS、Webブラウザ、JAM、
5 J a v a - A P、ネイティブAP等が行う動作は移動機16の動作となることから、以降の説明では、動作の主体を移動機16とする。

また、図9に示されるように、管理サーバ装置18の不揮発性メモリ18Aには、リストファイル200とSDF204が記憶されているものとする。これらはIPサーバ装置13およびIPサーバ装置14を管理するIPと管理サーバ装置18を管理する通信事業者との間で結ば
10 れた契約に従って通信事業者により作成されている。

これらのうち、リストファイル200は、移動機16において解釈・実行されると図10に示されるリストページ201を提供するように記述されている。また、リストファイル200は、リストページ201
15 を構成する選択肢201Aが押下されると（クリックまたはプレスされると）、後述の説明ファイル202のURL（“http://www.main.bbb.co.jp/ghi.html”）をGETメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。さらに、リストファイル200は、リストページ201を構成する選択
20 肢201Bが押下されると（クリックまたはプレスされると）、後述の説明ファイル207のURL（“http://www.ccc.co.jp/jkl.html”）をGETメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。

また、SDF204は、APIDとして“0001”、ポリシー情報として図4に示される内容の情報、有効期限として“2002年10月1日
25 午前10時”を内包しており、これらは通信事業者の秘密鍵を用いて署名されている。

また、IPサーバ装置12の不揮発性メモリ12Aには、「詰め将棋」なる名称のJ a v a - A Pソフトウェア（これを、本動作例では、第1

24

の非トラステッドＪａｖａ－ＡＰソフトウェアとする）に対応する説明
ファイル２１１、ＡＤＦ２１３およびＪａｒファイル２１４が記憶され
ているものとする。これらはＩＰサーバ装置１２を管理するＩＰによつ
て作成されている。これらのうち、説明ファイル２１１の内容は図１１
5 5 に示される通りであり、移動機１６において解釈・実行されると図１２
に示される説明ページ２１２を提供するように記述されている。また、
ＡＤＦ２１３はパッケージＵＲＬとしてＪａｒファイル２１４のＵＲ
Ｌ（“http://www.ccc.co.jp/shogi.jar”）を内包している。

また、ＩＰサーバ装置１２の不揮発性メモリ１２Ａには、「星占い」
10 なる名称のＪａｖａ－ＡＰソフトウェア（これを、本動作例では、第２
の非トラステッドＪａｖａ－ＡＰソフトウェアとする）に対応する説明
ファイル２０７、ＡＤＦ２０９およびＪａｒファイル２１０が記憶され
ているものとする。これらはＩＰサーバ装置１２を管理するＩＰによつ
て作成されている。これらのうち、説明ファイル２０７の内容は図１３
15 15 に示される通りであり、移動機１６において解釈・実行されると図１４
に示される説明ページ２０８を提供するように記述されている。また、
ＡＤＦ２０９はパッケージＵＲＬとしてＪａｒファイル２１０のＵＲ
Ｌ（“http://www.ccc.co.jp/horoscope.jar”）を内包している。

なお、上述した第１の非トラステッドＪａｖａ－ＡＰソフトウェアと
20 第２の非トラステッドＪａｖａ－ＡＰソフトウェアの違いは、後者に関
連する情報がリストファイル２００に登録されているのに対し、前者に
関連する情報が登録されていない点にある。

また、ＩＰサーバ装置１３の不揮発性メモリ１３Ａには、「電話帳ビ
ューア」なる名称のＪａｖａ－ＡＰソフトウェア（これを、本動作例で
25 25 はトラステッドＪａｖａ－ＡＰソフトウェアとする）に対応する説明フ
ァイル２０２、ＡＤＦ２０５およびＪａｒファイル２０６が記憶されて
いるものとする。これらはＩＰサーバ装置１３およびＩＰサーバ装置１
４を管理するＩＰによつて作成されている。これらのうち、説明ファイ
ル２０２の内容は図１５に示される通りであり、移動機１６において解

釈・実行されると図 16 に示される説明ページ 203 を提供するように記述されている。ADF 205 は、API D として “0001”、ハッシュ値として J a r ファイル 206 のハッシュ値、パッケージ URL として J a r ファイル 206 の U R L (“http://www.main.bbb.co.jp/viewer.jar”)、S D F - U R L として S D F 204 の U R L (“http://www.aaa.co.jp/viewer.sdf”)、及び通信事業者の公開鍵を内包している。また、移動機 16 は上述の各 J a v a - A P ソフトウェアをインストール可能な状態にあるものとする。

10 (3-1) インストール動作

まず、J a v a - A P ソフトウェアを移動機 16 にインストールする場合の動作例について、上述した J a v a - A P ソフトウェア毎に説明する。

(3-1-1) 第 1 の非トラステッド J a v a - A P ソフトウェア

15 第 1 の非トラステッド J a v a - A P ソフトウェアのインストール動作は、ユーザが移動機 16 を操作し、説明ファイル 211 の取得を試みることから始まる。これにより、移動機 16 では、説明ファイル 211 の U R L (“http://www.ccc.co.jp/mno.html”) を G E T メソッドのパラメータとして含む要求メッセージ t m 1 2 が生成される。この要求メッセージ t m 1 2 は、図 17 に示されるように、移動機 16 から送信され I P サーバ装置 12 により受信される。

I P サーバ装置 12 では、この要求メッセージ t m 1 2 の内容に対応して説明ファイル 211 を内包した応答メッセージ t m 1 3 が生成される。この応答メッセージ t m 1 3 は I P サーバ装置 12 から送信され移動機 16 により受信される。移動機 16 では、ユーザに対して、説明ファイル 211 の内容に応じた U I が提供される。この結果、表示部 16 C には、例えば図 12 に示すような説明ページ 212 が表示される。

この説明ページ 212 を見たユーザが、説明ページ 212 内のアンカー 212 A が押下されるよう移動機 16 を操作すると、移動機 16 では、

図 1 1 の説明ファイル 2 1 1 に記述されたアンカータグ（“<A” で始まるタグ）の i j a m 属性に指定されている値が i d 属性に指定されているオブジェクトタグ（“<OBJECT” で始まるタグ）が特定され、このオブジェクトタグの d a t a 属性に指定されている U R L
5 （“http://www.ccc.co.jp/shogi.jam”）が抽出され、この U R L で特定される A D F 2 1 3 の送信を要求する内容の要求メッセージ t m 1 6 が生成される。この要求メッセージ t m 1 6 は移動機 1 6 から送信され I P サーバ装置 1 2 により受信される。

I P サーバ装置 1 2 では、この要求メッセージ t m 1 6 の内容に対応
10 して A D F 2 1 3 を内包した応答メッセージ t m 1 7 が生成される。この応答メッセージ t m 1 7 は I P サーバ装置 1 2 から送信され移動機 1 6 により受信される。

移動機 1 6 では、A D F 2 1 3 の内容に基づいて第 1 の非トラステッド J a v a - A P ソフトウェアをインストール可能か否かが判定される。前述のように、移動機 1 6 は非トラステッド J a v a - A P ソフト
15 ウェアをインストール可能な状態にあるから、移動機 1 6 では第 1 の非トラステッド J a v a - A P ソフトウェアをインストール可能と判定される。

次に、移動機 1 6 では、A D F 2 1 3 が不揮発性メモリ 1 6 D に書き
20 込まれる。また、移動機 1 6 では、A D F 2 1 3 からパッケージ U R L （“http://www.ccc.co.jp/shogi.jar”）が抽出され、このパッケージ U R L で特定される J a r ファイル 2 1 4 の送信を要求する内容の要求メッセージ t m 1 8 が生成される。この要求メッセージ t m 1 8 は移動機 1 6 から送信され I P サーバ装置 1 2 により受信される。

I P サーバ装置 1 2 では、この要求メッセージ t m 1 8 の内容に対応
25 して J a r ファイル 2 1 4 を内包した応答メッセージ t m 1 9 が生成される。この応答メッセージ t m 1 9 は I P サーバ装置 1 2 から送信され移動機 1 6 により受信される。移動機 1 6 では J a r ファイル 2 1 4 が不揮発性メモリ 1 6 D に起動可能な状態で書き込まれ、これにより、

第1の非トラステッドJ a v a - A Pソフトウェアのインストールが完了する。

5 なお、移動機16において第1の非トラステッドJ a v a - A Pソフトウェアをインストール可能ではないと判断された場合、移動機16の状態はA D F 2 1 3の取得を開始する前の状態に戻る。

 (3-1-2) 第2の非トラステッドJ a v a - A Pソフトウェア

 第2の非トラステッドJ a v a - A Pソフトウェアのインストール動作は、ユーザが移動機16を操作し、説明ファイル207またはリストファイル200の取得を試みることから始まる。説明ファイル207
10 の取得を試みることから始まる動作はリストファイル200の取得を試みることから始まる動作のサブセットになっていることから、ここでは、リストファイル200の取得を試みることから始まる動作のみについて説明する。

 図18に示されるように、移動機16では、リストファイル200の
15 U R L ("http://www.aaa.co.jp/def.html") をG E Tメソッドのパラメータとして含む要求メッセージt m 2 0が生成される。この要求メッセージt m 2 0は移動機16から送信され管理サーバ装置18により受信される。

 管理サーバ装置18では、この要求メッセージt m 2 0の内容に対応
20 してリストファイル200を内包した応答メッセージt m 2 1が生成される。この応答メッセージt m 2 1は管理サーバ装置18から送信され移動機16により受信される。移動機16では、応答メッセージt m 2 1の受信を契機として、応答メッセージt m 2 1内のリストファイル200がHTMLに従って解釈され、移動機16のユーザに対して、
25 リストファイル200の内容に応じたU Iが提供される。この結果、移動機16の表示部16Cには、例えば図10に示すようなリストページ201が表示される。

 このリストページ201を視たユーザが、リストページ201内の選択肢201Bが押下されるように移動機16を操作すると、移動機16

では、選択肢 201B に対応付けられている URL
（“http://www.ccc.co.jp/jkl.html”）を GET メソッドのパラメータとして含む要求メッセージ t m 2 2 が生成される。この要求メッセージ t m 2 2 は移動機 16 から送信され IP サーバ装置 12 により受信
5 される。

IP サーバ装置 12 では、この要求メッセージ t m 2 2 の内容に対応して説明ファイル 207 を内包した応答メッセージ t m 2 3 が生成される。この応答メッセージ t m 2 3 は IP サーバ装置 12 から送信され移動機 16 により受信される。移動機 16 では、ユーザに対して、説明
10 ファイル 207 の内容に応じた UI が提供される。この結果、表示部 16C には、例えば図 14 に示すような説明ページ 208 が表示される。

この説明ページ 208 を見たユーザが、説明ページ 208 内のアンカー 208A が押下されるよう移動機 16 を操作すると、移動機 16 では、図 13 の説明ファイル 207 に記述されたアンカータグ（“<A” で始まるタグ）の i j a m 属性に指定されている値が i d 属性に指定されているオブジェクトタグ（“<OBJECT” で始まるタグ）が特定され、このオブジェクトタグの d a t a 属性に指定されている URL
15 （“http://www.ccc.co.jp/horoscope.jam”）が抽出され、この URL で特定される A D F 209 の送信を要求する内容の要求メッセージ t
20 m 2 6 が生成される。この要求メッセージ t m 2 6 は移動機 16 から送信され IP サーバ装置 12 により受信される。

IP サーバ装置 12 では、この要求メッセージ t m 2 6 の内容に対応して A D F 209 を内包した応答メッセージ t m 2 7 が生成される。この応答メッセージ t m 2 7 は IP サーバ装置 12 から送信され移動機
25 16 により受信される。

移動機 16 では、A D F 209 の内容に基づいて第 2 の非トラステッド J a v a - A P ソフトウェアをインストール可能か否かが判定される。前述のように、移動機 16 は第 2 の非トラステッド J a v a - A P ソフトウェアをインストール可能な状態にあるから、移動機 16 では非

トラステッドJ a v a - A P ソフトウェアをインストール可能と判定される。

次に、移動機16では、ADF209が不揮発性メモリ16Dに書き込まれる。また、移動機16では、ADF209からパッケージURL
5 (“http://www.ccc.co.jp/horoscope.jar”) が抽出され、このパッケージURLで特定されるJ a r ファイル210の送信を要求する内容の要求メッセージtm28が生成される。この要求メッセージtm28は移動機16から送信されIPサーバ装置12により受信される。

IPサーバ装置12では、この要求メッセージtm28の内容に対応
10 してJ a r ファイル210を内包した応答メッセージtm29が生成される。この応答メッセージtm29はIPサーバ装置12から送信され移動機16により受信される。移動機16ではJ a r ファイル210が不揮発性メモリ16Dに起動可能な状態で書き込まれ、これにより、第2の非トラステッドJ a v a - A P ソフトウェアのインストールが
15 完了する。

なお、移動機16において、第2の非トラステッドJ a v a - A P ソフトウェアをインストール可能ではないと判断された場合、移動機16の状態は、ADF209の取得を開始する前の状態に戻る。

(3-1-3) トラステッドJ a v a - A P ソフトウェア

20 トラステッドJ a v a - A P ソフトウェアのインストール動作は、ユーザが移動機16を操作し、説明ファイル202またはリストファイル200の取得を試みることから始まる。説明ファイル202の取得を試みることから始まる動作はリストファイル200の取得を試みることから始まる動作のサブセットになっていることから、説明ファイル20
25 2の取得を試みることから始まる動作についての説明を省略する。

図19に示されるように、リストファイル200の取得を試みることから始まる動作において、移動機16が応答メッセージtm21を受信し、例えば図10に示すようなリストページ201が表示されるまでは図18に示す動作と同一の動作が行われる。このリストページ201を

視たユーザが、リストページ201内の選択肢201Aが押下されるように移動機16を操作すると、移動機16では、選択肢201Aに対応付けられているURL（“http://www.main.bbb.co.jp/ghi.html”）をGETメソッドのパラメータとして含む要求メッセージtm32が生成される。この要求メッセージtm32は移動機16から送信されIPサーバ装置13により受信される。

IPサーバ装置13では、この要求メッセージtm32の内容に対応して説明ファイル202を内包した応答メッセージtm33が生成される。この応答メッセージtm33はIPサーバ装置13から送信され移動機16により受信される。移動機16では、ユーザに対して、説明ファイル202の内容に応じたUIが提供される。この結果、表示部16Cには、例えば図16に示すような説明ページ203が表示される。

この説明ページ203を視たユーザが、説明ページ203内のアンカー203Aが押下されるよう移動機16を操作すると、移動機16では、図15の説明ファイル202に記述されたアンカータグ（“<A”で始まるタグ）のijam属性に指定されている値がid属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）が特定され、このオブジェクトタグのdata属性に指定されているURL（“http://www.main.bbb.co.jp/viewer.jam”）が抽出され、このURLで特定されるADF205の送信を要求する内容の要求メッセージtm34が生成される。この要求メッセージtm34は移動機16から送信されIPサーバ装置13により受信される。IPサーバ装置13では、この要求メッセージtm34の内容に対応してADF205を内包した応答メッセージtm35が生成される。この応答メッセージtm35はIPサーバ装置13から送信され、ゲートウェイサーバ装置17及び移動パケット通信網15を介して移動機16により受信される。

移動機16において、ADF205は不揮発性メモリ16Dに書き込まれ、ADF205の内容に基づいてトラステッドJava-APソフトウェアをインストール可能か否かが判定される。前述のように、移動

機 1 6 は ト ラ ス テ ッ ド J a v a - A P ソ フ ト ウ ェ ア を イ ン ス ト ー ル 可
能 な 状 態 に あ る か ら、 移 動 機 1 6 で は ト ラ ス テ ッ ド J a v a - A P ソ フ
ト ウ ェ ア を イ ン ス ト ー ル 可 能 と 判 定 さ れ る。

そして、移動機 1 6 では、A D F 2 0 5 に 内 包 さ れ て い る S D F - U
5 R L “http://www.aaa.co.jp/viewer.sdf” で 特 定 さ れ る S D F 2 0 4
の 送 信 を 要 求 す る 内 容 の 要 求 メ ッ セ ー ジ t m 3 6 が 生 成 さ れ る。こ の 要
求 メ ッ セ ー ジ t m 3 6 は 移 動 機 1 6 か ら 送 信 さ れ 管 理 サ ー バ 装 置 1 8
に よ り 受 信 さ れ る。

管 理 サ ー バ 装 置 1 8 で は、こ の 要 求 メ ッ セ ー ジ t m 3 6 の 内 容 に 対 応
10 し て S D F 2 0 4 を 内 包 し た 応 答 メ ッ セ ー ジ t m 3 7 が 生 成 さ れ る。こ
の 応 答 メ ッ セ ー ジ t m 3 7 は 管 理 サ ー バ 装 置 1 8 か ら 送 信 さ れ ゲ ー ト
ウ ェ イ 装 置 1 7 及 び 移 動 パ ケ ッ ト 通 信 網 1 5 を 介 し て 移 動 機 1 6 に よ
り 受 信 さ れ る。こ こ で、管 理 サ ー バ 装 置 1 8 と ゲ ー ト ウ ェ イ サ ー バ 装 置
1 7 と の 間 の 通 信 路 は 専 用 線 で あ り、ゲ ー ト ウ ェ イ サ ー バ 装 置 1 7 は セ
15 キ ュ リ テ ィ の 確 保 さ れ た 移 動 パ ケ ッ ト 通 信 網 1 5 に 直 接 的 に 接 続 さ れ
て い る こ と か ら、移 動 機 1 6 に 受 信 さ れ る ま で に S D F 2 0 4 が 改 竄 さ
れ る 虞 は 無 い。

さ ら に、移 動 機 1 6 で は、A D F 2 0 5 に 内 包 さ れ て い る 公 開 鍵 を 用
い て S D F 2 0 4 の 正 当 性 が 判 断 さ れ る。前 述 の よ う に、A D F 2 0 5
20 に 内 包 さ れ て い る 公 開 鍵 は S D F 2 0 4 へ の 署 名 の 際 に 用 い た 秘 密 鍵
と 対 応 し て い る こ と か ら、管 理 サ ー バ 装 置 1 8 内 に お い て S D F 2 0 4
の 内 容 が 変 更 さ れ て い な い 限 り、S D F 2 0 4 が 正 当 で あ る と 判 断 さ れ
る。

S D F 2 0 4 が 正 当 で あ る と 判 断 さ れ る と、移 動 機 1 6 で は、A D F
25 2 0 5 に 内 包 さ れ て い る A P I D と S D F 2 0 4 に 内 包 さ れ て い る A
P I D と が 比 較 さ れ る。前 述 の よ う に、I P サ ー バ 装 置 1 3 に お け る A
D F 2 0 5 に は S D F 2 0 4 内 の A P I D と 一 致 す る A P I D が 記 述
さ れ る よ う に 定 め ら れ て い る こ と か ら、記 述 ミ ス 等 が 無 い 限 り、A D F
2 0 5 に 内 包 さ れ て い る A P I D と S D F 2 0 4 に 内 包 さ れ て い る A

P I Dは一致する。次いで、移動機 1 6 では、S D F 2 0 4 が不揮発性メモリ 1 6 Dに書き込まれる。

次に、移動機 1 6 では、A D F 2 0 5 からパッケージU R L
(“http://www.main.bbb.co.jp/viewer.jar”) が抽出され、このパッ
5 ケージU R Lで特定されるJ a r ファイル2 0 6 の送信を要求する内
容の要求メッセージt m 3 8 が生成される。この要求メッセージt m 3
8 は移動機 1 6 から送信されI Pサーバ装置 1 3 により受信される。

I Pサーバ装置 1 3 では、この要求メッセージt m 3 8 の内容に対応
してJ a r ファイル2 0 6 を内包した応答メッセージt m 3 9 が生成
10 される。この応答メッセージt m 3 9 はI Pサーバ装置 1 3 から送信さ
れ移動機 1 6 により受信される。

次に、移動機 1 6 ではJ a r ファイル2 0 6 と所定のハッシュ関数と
を用いてハッシュ値が算出され、このハッシュ値とA D F 2 0 5 に内包
されているハッシュ値とが比較される。前述のように、A D F 2 0 5 に
15 はこのA D F 2 0 5 に対応するJ a r ファイルのハッシュ値が記述さ
れるように定められていることから、記述ミス等がない限り、両ハッ
シュ値は一致する。

両ハッシュ値が一致すると、移動機 1 6 では、J a r ファイル2 0 6
が不揮発性メモリ 1 6 Dに起動可能な状態で書き込まれ、これにより、
20 トラステッドJ a v a - A Pソフトウェアのインストールが完了する。

なお、移動機 1 6 においてS D F 2 0 4 が正当でないと判断された場
合や、A D F 2 0 5 に内包されているA P I DとS D F 2 0 4 に内包さ
れているA P I Dが不一致の場合、トラステッドJ a v a - A Pソフト
ウェアをインストール可能ではないと判断された場合、算出したハッ
25 シュ値とA D F 2 0 5 に内包されているハッシュ値とが不一致の場合に
は、移動機 1 6 の状態はA D F 2 0 5 の取得を開始する前の状態に戻る。

(3 - 2) J a v a - A Pソフトウェアが起動されている時の移動機 1
6 の挙動

次に、上述の各々のJ a v a - A Pソフトウェアが起動されている時

の移動機 16 の挙動について説明する。

(3-2-1) 非トラステッド J a v a - A P ソフトウェアの挙動

上述したインストール動作により移動機 16 にインストールされた非トラステッド J a v a - A P ソフトウェア (第 1 の非トラステッド J a v a - A P ソフトウェア (詰め将棋) 及び第 2 の非トラステッド J a v a - A P ソフトウェア (星占い) の双方を含む) が、J A M が実現された移動機 16 において起動され、このソフトウェアに対応した機能 (以後、非トラステッド J a v a - A P) が移動機 16 内に実現されたときの移動機 16 の挙動について説明する。

10 非トラステッド J a v a - A P が使用しようとする A P I が非トラステッド A P I の場合、前述したように非トラステッド A P I はあらゆる J a v a - A P の使用が許可されているから、この場合の A P I の使用は J A M により許可されることとなる。したがって、非トラステッド J a v a - A P はこの非トラステッド A P I を使用することができる。

15 また、非トラステッド J a v a - A P が使用しようとする A P I がトラステッド A P I の場合、J A M はこの J a v a - A P に対応する S D F が不揮発性メモリ 16 D に記憶されているか否かを調べる。ここでは、そのような S D F は不揮発性メモリ 16 D に記憶されていないから、J A M は非トラステッド J a v a - A P によるこの A P I の使用を禁止する。したがって、非トラステッド J a v a - A P はトラステッド A P I を使用することができない。

(3-2-2) トラステッド J a v a - A P ソフトウェアの挙動

25 移動機 16 にインストールされたトラステッド J a v a - A P ソフトウェア (電話帳ビューワ) が、J A M が実現された移動機 16 において起動され、このソフトウェアに対応した機能が移動機 16 内に実現されたときの移動機 16 の挙動について説明する。

トラステッド J a v a - A P が使用しようとする A P I が非トラステッド A P I の場合、前述したように、この A P I の使用は J A M によって当然許可される。したがって、トラステッド J a v a - A P はこの

非トラステッドAPIを使用することができる。

トラステッドJava-APが使用しようとするAPIがトラステッドAPIの場合、このJava-APに対応するSDFが不揮発性メモリ16Dに記憶されているので、このAPIの使用はJAMによって許可され得るが、そのトラステッドJava-APの挙動はSDF内のポリシー情報に依存する。以下、使用するAPI毎にその挙動について説明する。

(3-2-2-1) getPhoneList()

“getPhoneList()”はトラステッドAPIであるから、このAPIの使用の可否は、不揮発性メモリ16Dに記憶されているSDF204内のポリシー情報に基づいてJAMにより決定される。このポリシー情報の内容は図4に示される通りであることから、“getPhoneList()”の使用がJAMにより許可される。したがって、トラステッドJava-AP（電話帳ビューワ）は“getPhoneList()”を使用することができる。つまり、このトラステッドJava-APは電話帳データを読み出すことができる。

(3-2-2-2) getCallHistory()

“getCallHistory()”はトラステッドAPIであるから、このAPIの使用の可否はSDF204内のポリシー情報に基づいてJAMにより決定される。このポリシー情報の内容は図4に示される通りであることから、“getCallHistory()”の使用がJAMにより禁止される。したがって、トラステッドJava-AP（電話帳ビューワ）は“getCallHistory()”を使用することができない。つまり、このトラステッドJava-APは発着信履歴データを読み出すことができない。

(3-3) トラステッドJava-APソフトウェアの有効期限更新時の動作

次に、トラステッドJava-APソフトウェアの有効期限を更新する動作例について説明する。以下の説明においては、図9において、管理サーバ装置18内においてSDF204がSDF204aに更新さ

れているものとする。ただし、その更新内容は、有効期限が“2002年10月1日午前10時”から“2003年1月1日午前10時”に変更されたということのみであり、SDF204とSDF204aの記憶位置やそのファイル名、署名に用いた秘密鍵等は一切変更されていないものとする。

移動機16は、計時部16Hによって計時される現在日時と、今までに取得した全てのSDFに内包されている複数の有効期限とを常時監視しており、有効期限が到来したか否かを判断している。ここで、計時部16Hによって計時される現在日時が2002年10月1日午前10時となったとき、APID“0001”に対応するトラステッドJava-APソフトウェア（電話帳ビューワ）の有効期限が到来することとなり、これによって、図20に示す動作が開始される

まず、移動機16は、図21に示すように、有効期限が到来したトラステッドJava-APソフトウェアの名称“電話帳ビューワ”とともに、有効期限が到来したので更新するか否かをユーザに問い合わせるメッセージを表示部16cに表示してユーザの操作があるまで待機する。

ここで、ユーザが有効期限を更新することを指示する操作を行うと、移動機16はこの指示内容を解釈し、APID“0001”を内包したADFに内包されているSDF-URL（“http://www.aaa.co.jp/viewer.sdf”）をGETメソッドのパラメータとして含む要求メッセージtm41を生成する。この要求メッセージtm41は移動機16から送信され管理サーバ装置18により受信される。

管理サーバ装置18では、この要求メッセージtm41の内容に対応してSDF204aを内包した応答メッセージtm42が生成される。この応答メッセージtm42は管理サーバ装置18から送信され移動機16により受信される。

一方、移動機16は、上記SDF-URLを用いてSDF204aを取得できたか否かを判断する。ここでは取得に成功することを想定して

いるので処理は次に進み、移動機16は、SDF204aの署名を、既に取得しているADF205に内包されている公開鍵を用いて検証し（復号し）、このSDF204aの正当性を判断する。正当性が確認されると（ステップS35；Yes）、移動機16は、SDF204aから抽出したAPIDと既に取得済みのADF205に内包されていたAPIDとを比較し、両者が一致するか否かを判定する。

ここでは両者が一致するはずなので、移動機16は、不揮発性メモリ16Dに記憶されているSDF203をSDF204aで上書きし、これにより、トラステッドJava-APソフトウェア（電話帳ビューワ）の有効期限が“2002年10月1日午前10時”から“2003年1月1日午前10時”に更新される。

なお、ユーザの操作により有効期限を更新しないと判断された場合、SDFを取得できなかった場合、SDFが正当でないと判断した場合、SDFが有するAPIDとADFが有するAPIDが不一致の場合、JAMは、有効期限を更新しない旨をユーザに通知するとともに、移動機16の状態をSDF203aを取得する以前の状態に戻す。

（3-4）トラステッドJava-APソフトウェアの変更後の動作

次に、IPサーバ装置13およびIPサーバ装置14を管理するIPがトラステッドJava-APソフトウェアの配信形態や内容を変更した場合の本システム動作について説明する。ただし、ここでの変更は、トラステッドJava-APソフトウェアの改善等を目的としたJarファイル206の内容の変更と、IPサーバ装置13の負荷の軽減等を目的とした配信形態の変更とを含む。後者の変更を達成するために、IPサーバ装置13およびIPサーバ装置14を管理するIPは、図22に示すように、変更後のJarファイル206（以後、Jarファイル215）をIPサーバ装置14の不揮発性メモリ14Aに記憶させ、このJarファイル215に対応するようにADF205の内容を変更してADF216としている。変更後のトラステッドJava-APソフトウェアの配信に必要な作業は以上の通りであり、管理サーバ装置

18を管理する通信事業者が行うべき作業は存在しない。つまり、通信事業者はリストファイル200やSDF204を変更する必要はない。

このような変更の後のトラステッドJava-APソフトウェアのインストール動作は、図23に示す通りとなる。この図に示す動作が図19に示す動作と相違し始めるのは、移動機16がJarファイルを要求する時点からである。なお、両図において、応答メッセージtm47は応答メッセージtm37、要求メッセージtm48は要求メッセージtm38、応答メッセージtm49は応答メッセージtm39に対応している。

即ち、図23において図19に示す動作と本質的に異なるのは、ADF216およびJarファイル215が処理の対象となる点と、ADF216に内包されているパッケージURL（“http://www.sub.bbb.co.jp/viewer.jar”）で特定されるJarファイル215の送信を要求する内容の要求メッセージtm48が移動機16にて生成される点と、この要求メッセージtm48が移動機16から送信されIPサーバ装置14により受信される点と、IPサーバ装置14においてJarファイル215を内包した応答メッセージtm49が生成される点と、この応答メッセージtm49がIPサーバ装置14から送信され移動機16により受信される点のみである。

以上説明したように、移動機16においては、ダウンロードしたSDFに含まれるポリシー情報の内容に応じた挙動がこのSDFに対応するトラステッドJava-APソフトウェアに許可され、ポリシー情報の内容に含まれていない挙動は許可されない。このポリシー情報は管理サーバ装置18からセキュリティが確保された上で移動機16へ送信されるから、ポリシー情報が第三者により改竄される虞もなく、これにより、トラステッドJava-APの信頼性が確保される。また、ユーザから視れば、従来通りの非トラステッドJava-APの他に、上記のような、より自由な挙動が許可されたトラステッドJava-APを利用可能となり、非常に便利である。

なお、上述の配信システムにおいては、移動機 16 に対し、ADF、SDF、Jar ファイルという順序で各種ファイルの配信を行っていたが、このような順序で配信することにより、以下のような効果が生ずる。

既に説明したように、Java-AP ソフトウェア (ADF 及び Jar
5 r ファイル) は IP によって設計・作成され、各々の IP がインターネット上に開設している専用サイト (図 1 の IP サーバ装置 12 ~ 14) において、一般ユーザに公開されている。従って、ユーザはまず、IP の専用サイトにアクセスし、そこで、様々な Java-AP ソフトウェアの解説ページを参照してそのソフトウェアをダウンロードをするか
10 否かを判断するのが普通である。そして、ユーザは Java-AP ソフトウェアをダウンロードしよう判断すると、そのダウンロード処理を指示する操作を行う必要があるが、そのために上記の解説ページには次にダウンロードすべきファイルの URL がアンカータグによって埋め込まれているのが普通である。このとき、IP の立場から視れば、解説
15 ページに ADF の URL を埋め込むのが最も手間がかからない。なぜなら、ADF は IP の管理下にあるので、その ADF の URL は IP によって常に把握できているからである。これに対し、解説ページに SDF の URL を埋め込むとなると、IP は通信事業者に問い合わせをする等して、URL の正誤の確認処理を絶えず欠かさないようにしなければならない。よって、ADF、SDF、Jar ファイルという順序で各種フ
20 ァイルの配信を行うことは非常に有意義である。

また、上記の順序は、エヌティティドコモ社の i モード (登録商標) において現在実施されている Java-AP ソフトウェアのバージョンアップ処理を考慮した場合にも利点がある。現状の i モードのサービ
25 ス仕様においては、ユーザによってバージョンアップを要求する操作がなされると、移動機は、まず、ADF に記述された内容を参照し、ADF に記述されたパッケージ URL に基づいて、バージョンアップ後の Jar ファイルを取得するようになっている。即ち、バージョンアップ時には、まず ADF を参照してから、その後にダウンロード処理に移行す

るようになっている。この点を考慮すると、本実施形態の配信システムにおけるバージョンアップ時においても、まずADFを参照し、そのADFに記述されているSDF-URLに基づいてSDFを取得した後、Jarファイルを取得するというように、まずADFの参照から一連の

5 処理を開始すると、それ以降は、SDF→Jarファイルという通常のダウンロードと同じ流れで処理を行うことができ、現状のサービス仕様をあまり変更しないで済む。これに対し、仮にSDF、ADF、Jarファイルという順序で各種ファイルをダウンロードすることが定義付けられている場合、バージョンアップしようとした場合、ADFを参照

10 からダウンロード処理を開始すると、SDFを取得することなくJarファイルの取得処理にまで至ってしまう。SDFは、バージョンアップ時に書き換えられることは十分にあり得るので、SDFが無いとセキュリティ上で不都合が生ずるおそれがある。以上のような観点からも、ADF、SDF、Jarファイルという順序で各種ファイルの配信を行う

15 ことは有意義である。

(3) 変形例

本発明は上述した実施形態に限定されず、以下のような種々の変更が可能である。

上述した配信システムでは、移動機は、秘密鍵による署名データと公開鍵とを用いてSDFとADFの作成者との対応関係の正当性を確認

20 するようにした。しかし、これに限らず、SDFとADFの作成者との対応関係の正当性が確認できる方式であればどのような方式を用いてもよい。

また、システムに要求されるセキュリティレベルによっては、SDF

25 に公開鍵を内包させず、IPサーバ装置においてはADFに対する秘密鍵を用いた署名を行わず、かつ移動機においてはこの確認処理を省略する、という形態とし、移動機およびIPサーバ装置における処理量や、移動機と管理サーバ装置およびIPサーバ装置との間の通信量を低減するようにしてもよい。

また、上述した配信システムでは、J a r ファイルのハッシュ値をこの J a r ファイルに対応する A D F に内包させる一方、移動機において J a r ファイルのハッシュ値を生成し、これら両者を比較して J a r ファイルと A D F との対応関係の正当性を確認するようにしていた。しかし、これに限らず、J a r ファイルと A D F との対応関係の正当性が確認できる方式であればどのような方式を用いてもよい。

また、システムに要求されるセキュリティレベルによっては、A D F にハッシュ値を内包させずにこの確認処理を省略する形態とし、移動機および I P サーバ装置における処理量や移動機と I P サーバ装置との間の通信量を低減するようにしてもよい。

また、上述した配信システムでは、トラステッド J a v a - A P に固有の A P I D を使用して S D F と A D F （および J a r ファイル）との対応が正当であるか否かを判定するようにしたが、トラステッド J a v a - A P を提供する情報提供事業者に固有の C I D を用いて S D F と A D F （および J a r ファイル）との対応が正当であるか否かを判定するようにしてもよい。また、システムに要求されるセキュリティレベルによっては、A P I D や C I D を用いた判定を省略するようにしてもよい。

また、上述した配信システムではドメインネームを用いてサーバを指定するようにしたが、I P アドレスを用いてサーバを指定するようにしてもよい。

また、移動機において、A D F に内包されている S D F - U R L のうちのドメインネームを予め設定された文字列と比較し、信頼できる機関が管理するサーバ装置のドメインネームである場合にのみ、S D F を正当と認める態様としてもよい。この場合、予め設定された文字列と異なるときは、移動機 1 6 は、S D F 取得に失敗した旨を表示し、管理サーバ 1 8 に S D F を要求せずに処理を終了することとなる。

また、この態様では、比較対象の文字列（例えば、通信事業者のドメインネームを示す文字列）は移動機の R O M または不揮発性メモリに予

め格納されることになる。ROMに予め格納する態様では、文字列の書き換えが不可能であるから、より高いセキュリティを確保できる。また、不揮発性メモリに予め格納する態様では、移動機の売買後に信頼できる機関を格納することができるので、ユーザおよび信頼できる機関に対して優れた利便性を提供することができる。

また、上述した配信システムでは、SDFの配信に使用する通信路を提供する通信事業者を信頼できる機関として高いセキュリティを確保するようにしたが、本発明は通信路の提供が信頼できる機関により為されていない態様をも技術的範囲に含む。例えば、信頼できる機関と移動機とを暗号化通信路により接続し、この通信路を介して信頼できる機関がSDFを配信するようにしてもよい。また、通信路のセキュリティが確保されていなくても、SDFを暗号化した後に配信し、移動機においてSDFを復号するようにすれば、ある程度のセキュリティを確保してSDFを配信することができる。

上述した配信システムでは、HTTPに従ってファイルを送受するようにしたが、HTTPSを使用し、より高いセキュリティを確保するようにシステムを変形してもよい。

また、上述した配信システムにおいて、信頼できる機関がIPとなつてよいこと、すなわち、管理サーバ装置がIPサーバ装置を兼ねるようにしてもよいことは言うまでもない。

さらに、上述した配信システムでは、Java-APによる利用を制限する対象としてAPIを挙げたが、本発明はこれに限定されるものではなく、任意の資源（リソース）を対象とすることができる。ここでいう資源はハードウェア資源であってもよいし、後述するネットワーク資源やソフトウェア資源であってもよい。ハードウェア資源としては、メモリやスピーカ、マイク、赤外線コントローラ、LED（Light Emitting Diode）等の移動機が備え得るものや、移動機と共働し得るUIM（User Identity Module）やSIM（Subscriber Identity Module）等の外部機器なども挙げられる。

次にネットワーク資源について説明する。前述したように、移動機は移動通信網との間で無線通信を行う。この無線通信時には、移動機は、移動通信網により提供される無線チャネル等の無線資源を使用する。この無線資源はネットワーク資源の一種である。また、移動機は無線資源が属する通信プロトコルレイヤよりも高位の通信プロトコルレイヤにおいて、パケットの伝送路や回線接続の通信路などの通信資源を使用する。このような通信資源もネットワーク資源の一種である。

次にソフトウェア資源について説明する。ソフトウェア資源としては、API やクラス、パッケージ等が挙げられる。ソフトウェア資源が提供する機能は様々であるが、典型的な機能として、暗号演算などの演算処理機能や、Web ブラウザ等の他のアプリケーションとの間でデータを送受したりする機能などが挙げられる。また、本発明は、上記外部機器が有するソフトウェア資源をも利用の制限対象とする態様を技術的範囲に含む。

ところで、Java-AP によるハードウェア資源やネットワーク資源の利用は、ソフトウェア資源を利用して行われるのが一般的である。上述した配信システムにおける移動機も、ハードウェア資源やネットワーク資源を利用するためのソフトウェア資源を有しており、このようなソフトウェア資源の利用を制限することにより、間接的に、ハードウェア資源やネットワーク資源の利用を制限している。このように、間接的な制限の形態としたことにより、多様なソフトウェア資源を用意すれば、Java-AP のうちのトラステッド Java-AP についてのみ、自他の Java-AP の権限を変更する権限を与える、またはダウンロード元のサーバ装置としか通信することができないという制限を外す、あるいはメモリの特定の記憶領域に対してアクセスできるようにするといった、複数の資源の制限を細かく変更しなければ実現できないようなことまで容易に指定できるようになる。なお、移動機内部のソフトウェア資源の利用を制限して上記外部機器のソフトウェア資源の利用を間接的に制限する態様も本発明の技術的範囲に含まれる。

なお、パーミッションの表現方法としては、一つの資源と一つのフラグ（許可／禁止）とを対応付けるようにしてもよいし、複数の資源のパーミッションを一つの情報で示すようにしてもよい。

また、本発明では、複数の利用の種類を持つ資源について、利用を許可（あるいは禁止）する種類を示すようにパーミッションを設定することも可能である。この場合、移動機において、より木目細かな制御が実現される。例えば、メモリには読み出しと書き込みの2つの利用形態（利用の種類）があるから、非トラステッドJava-APには読み出しでしか利用されないが、トラステッドJava-APには読み出し及び書き込みの両方で利用され得るようにすることもできる。また、例えば、1つのパケット伝送路を複数のアプリケーションが共用可能な移動機において、パケット伝送路を利用する権限を有するJava-APが起動されている間にWebブラウザ等が起動された場合、このJava-APが「パケット伝送路の利用を排他的に行う」ことを許可されていないJava-APであればWebブラウザ等によるパケット伝送路の共用を排除することはできないが、「パケット伝送路の利用を排他的に行う」ことを許可されているJava-APであればパケット伝送路を占有して使用することができる、といった制御が可能となる。

さらに、この例を変形することで、ある種のパーミッションを与えられたJava-APはユーザに許可を求めることなくパケット通信路を排他的に利用することが可能であり、別のパーミッションを与えられたJava-APはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用するためにはユーザの許可を得ることが必要であり、さらに別のパーミッションを与えられたJava-APはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用することは不可能であり、さらに別のパーミッションを与えられたJava-APはユーザの許可を得て初めてパケット通信路を利用することが可能であり、さらに別のパーミッションを与えられたJava-APはパ

ケット通信路を利用することすらできない、といった制御も可能となる。この例から明らかなように、本発明における「利用の種類」には、資源を利用する際に経る手順の種類（ユーザの許可を得る手順／ユーザの許可を得ない手順）も含まれる。

- 5 また、上述した配信システムでは全ての移動機に対して同一のリストページが提供されるが、移動機毎に異なるリストページを提供するようにしてもよい。

- 10 また、上述の配信システムでは、J a v a - A P の実行時に J a v a - A P の挙動を制限するようにしたが、I P サーバ装置に格納されている J a r ファイルにポリシー情報を内包させ、J a r ファイルのダウンロード時に、移動機において、このポリシー情報と S D F 中とのポリシー情報とを比較し、両者が一致しない場合には、この J a r ファイルに対応する J a v a - A P を起動できないように、あるいはこの J a r ファイルを含む J a v a - A P ソフトウェアをインストールできないようにしてもよい。もちろん、両ポリシー情報の一致する項目についてのパーミッションのみを有効とするようにしてもよい。

- 15 通信事業者の公開鍵は、I P サーバ装置 1 2 ～ 1 4 から A D F に含めて移動機 1 6 に提供されるようになっていたが、これに限らず、予め移動機に格納されていてもよい。公開鍵は予め移動機に格納する方法としては、通信により配信し不揮発性メモリに書き込んでおく方法、R O M に書き込んだ後に移動機を販売する方法などが考えられる。

20 また、上述の配信システムではソフトウェアは移動機へ配信されるが、本発明の技術的範囲には、移動機以外の端末装置へ配信する態様も含まれる。

- 25 上述の配信システムでは、トラステッド J a v a - A P ソフトウェアの有効期限が到来したタイミングで、その有効期限を更新するための処理を開始していた。しかし、更新タイミングは上記のものに限らず、ユーザが所望する恣意的なタイミングや、毎月末 1 回等の定期的なタイミングというように、様々な態様を採用し得る。

また、有効期限の設定の仕方は、既に説明したように日時によって設定してもよいが、この他にも、例えばトラステッドJ a v a - A Pソフトウェアのダウンロード時からの期間（例えばダウンロードしてから1ヶ月のみ使用可能というような場合）によって設定してもよいし、トラ

5 ステッドJ a v a - A Pソフトウェアの実行回数や実行期間によって設定してもよい。要するに、有効期限とは、J a v a - A Pソフトウェアを無制限には実行できないようにその上限を定めた情報であればどのようなものであってもよい。

例えば実行回数で有効期限を設定した場合、トラステッドJ a v a - A Pソフトウェアの起動時にJ A MはS D F内のポリシー情報を参照するようになっているので、その参照回数をトラステッドJ a v a - A Pソフトウェアの実行回数としてカウントしてもよい。そして、カウントした実行回数が予め定められた数に達すると、その更新処理に移行すればよい。

10

また、トラステッドJ a v a - A Pソフトウェアが実行されている期間を累積してカウントするような手段（例えばそのトラステッドJ a v a - A Pソフトウェア内にサブルーチンとして記述する等の手段）を備えていれば、実行期間によって有効期限を設定した場合にも対応できる。そして、カウントした実行期間が予め定められた時間に達すると、その

15

20 更新処理に移行すればよい。

なお、上述の配信システムの説明では「トラステッドJ a v a - A Pソフトウェアの有効期限」という表現を用いていたが、より厳密には、J a rファイルそのものの有効期限であってもよいし、S D Fそのものの有効期限であってもよいし、その両者の有効期限であってもよいことはもちろんである。

25

また、上述の配信システムでは、有効期限が到来してもそれを更新できない場合、その有効期限が到来したトラステッドJ a v a - A Pソフトウェアを実行禁止となっていたが、これに限らず、その有効期限経過時にトラステッドJ a v a - A Pソフトウェアから非トラステッドJ

a v a - A P ソフトウェアに遷移させてもよい。即ち、有効期限が到来した J a v a - A P ソフトウェアは、非 J a v a - A P ソフトウェアであるとみなされ、その遷移後は、非トラステッド J a v a - A P ソフトウェアとしての、より厳しい挙動を制限を受けることとなる。

- 5 また、任意のトラステッド J a v a - A P ソフトウェアの S D F を失効させることができるように、上記実施形態を変形してもよい。

この変形例において、管理サーバは、上記実施形態と同様、各種の J a v a - A P ソフトウェアの S D F を記憶するための記憶部を有している。管理サーバの制御部は、通信部により各 S D F を受信し、あるい
10 は記憶媒体に格納された S D F を受け取ったとき、この記憶部に格納する。

また、管理サーバには、任意のトラステッド J a v a - A P ソフトウェアについて、その S D F を失効させる旨のコマンドが入力され得る。このコマンドは、失効させるべき S D F が帰属するトラステッド J a v
15 a - A P ソフトウェアの A P I D を含んでいる。このようなコマンドは、オペレータにより管理サーバの入力部に入力され、あるいは該当する I P サーバからネットワークを介して管理サーバ宛てに送信され、管理サーバの通信部によって受信される。管理サーバの制御部は、このコマンドを入力部あるいは通信部を介して受け取ると、コマンド中の A P I D
20 により特定される S D F が失効した旨の情報を記憶部に格納する。これにより、以後、管理サーバでは、この S D F の公開が停止され、この S D F を利用した J a v a - A P ソフトウェアのダウンロードが不可能になる。

ところで、あるトラステッド J a v a - A P ソフトウェアの S D F が、
25 ある端末装置に配信され、その後、その S D F が失効するような場合も考えられる。この場合、既に配信済みの S D F が S D F として機能しないようにするべきである。そこで、次のような方法が考えられる。すなわち、端末装置が S D F の有効性を例えば一定時間間隔で管理サーバに問い合わせ、S D F が失効している旨の応答が管理サーバから返ってき

たときにはそれ以降のSDFの使用を禁止するのである。ここで、SDFが失効になった後、トラステッドJava-APソフトウェアが実行される回数を減らすためには、問い合わせの時間間隔を短くするのが有効である。しかし、そのようなことを全端末装置について一律に行うと、

5 トラヒックが膨大になりユーザが負担する通信費もかさむ。一方、端末装置のユーザの中には、頻繁にトラステッドJava-APソフトウェアの実行を指示する人もいれば、たまにしか実行を指示しない人もいたので、後者の人のためにトラヒックおよび通信費を増やすのは得策ではない。

- 10 この問題を解決するため、本変形例では次のような処理が行われる。まず、管理サーバ装置は、SDFを通信部により端末装置に送信する際、頻度データNと間隔データTを含ませる。ここで、頻度データNは、トラステッドJava-APソフトウェアの実行回数がNの整数倍を越える毎にSDFの有効性についての問い合わせを送信することを指示
- 15 するデータである。また、間隔データTは、トラステッドJava-APソフトウェア実行終了後、次にJava-APソフトウェアの実行が開始される前に、時間Tが経過したとき、SDFの有効性についての問い合わせを送信することを指示するデータである。

- 20 端末装置は、あるSDFを受信した場合、そのSDF内の頻度データNおよび間隔データTに従って、そのSDFの有効性についての問い合わせを管理サーバ装置に送信する。図24には、1つのSDFについてこのような処理を行うための制御部の構成が示されている。端末装置が複数のSDFを記憶している場合には、図24に示すものが、これと同数だけ制御部内に用意されると考えて良い。なお、図24において符号
- 25 501～504によって示される要素は制御部を構成する回路あるいは制御部によって実行されるルーチンを表している。

まず、端末装置の制御部は、SDFを受信すると、図24に示す回路ないしルーチンをそのSDFのために活性化する。そして、SDFから頻度データNと間隔データTを取り出し、頻度データNを除算器502

に、間隔データTをタイマ503に設定する。

カウンタ501は、SDFに対応したトラステッドJava-APソフトウェアが起動される都度、1ずつカウント値を増す。除算器502は、カウンタ501のカウント値、即ちトラステッドJava-APソフトウェアの起動回数を頻度データNによって除算し、その除算結果の余りが1になったとき、信号“1”を出力する。

タイマ503は、具体的にはダウンカウンタである。トラステッドJava-APソフトウェアが起動されると、間隔データTがカウント値の初期値として503に書き込まれる。その後、タイマ503は、所定周波数のクロックに同期して、ダウンカウントを進める。そして、T相当の時間が経過し、タイムアウトになると、タイマ503は信号“1”を出力する。タイムアウト前にトラステッドJava-APソフトウェアが再起動されると、間隔データTがタイマ503にセットされ、その時点から新たなダウンカウントが始まる。

ORゲート504は、除算器502またはタイマ503から信号“1”が出力されると、SDFの有効性の問い合わせを指示する信号を発生する。

図25は、以上説明した動作を示すタイムチャートである。同図に示すとおり、頻度データNが与えられることにより、ORゲート504はN+1回目、2N+1回目という具合に、SDFの有効性の問い合わせを指示する信号を発生する。制御部は、この信号が発生したとき、SDFの有効性についての問い合わせを通信部により管理サーバ装置に送る。この問い合わせは、その対象であるSDFを特定するAPIDを含んでいる。管理サーバの制御部は、この問い合わせを通信部により受信すると、記憶部を参照することにより、問い合わせ中のAPIDにより特定されるSDFが有効であるか失効しているかを調べ、その結果を通信部により端末装置に回答する。端末装置の制御部は、問い合わせを行ったSDFが失効している旨の回答を通信部により受け取った場合、そのSDFに対応したJava-APソフトウェアが起動できないよう

制御を行う。

また、図 25 に示す例では、2 回目にトラステッド J a v a - A P ソフトウェアが実行された後、3 回目の実行の前に、経過時間が T を越えたため、S D F の有効性の問い合わせを指示する信号が発生している。

- 5 この場合も、上記と同様な問い合わせ、管理サーバからの応答、応答に応じた端末装置側の動作が行われる。

以上説明した本変形例の利点は次の点にある。

- 10 まず、頻繁にトラステッド J a v a - A P ソフトウェアを使用する人の場合、間隔データ T に基づく問い合わせ発生制御だけを行うと、常にタイムアウトになる前にトラステッド J a v a - A P ソフトウェアが起動されるため、問い合わせが行われない。従って、このようなユーザのためには、起動回数が N を越えたときに問い合わせるという方法が有効である。

- 15 一方、トラステッド J a v a - A P ソフトウェアをたまにしか使わない人の場合、なかなか起動回数が N を越えないので、タイムリーに S D F を失効させることができない。従って、このようなユーザのためには、起動後の経過時間が T を越えたときに問い合わせるという方法が有効である。

- 20 本変形例は、これら両方法を並列使用するので、両方のタイプの人に有効である。

請求の範囲

1. アプリケーションを実現するためのソフトウェアを内包した実体ファイル
を格納した情報提供サーバ装置と、端末装置が前記ソフトウェア
5 を実行することにより実現されるアプリケーションに与えられた権限
を示す権限情報を内包したセキュリティ記述ファイルを格納した管理
サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイル
の格納位置と前記セキュリティ記述ファイルの格納位置とが記述さ
れたアプリケーション記述ファイルを格納した情報提供サーバ装置と
10 を有した配信システムが、前記アプリケーション記述ファイルの格納位
置を前記端末装置によって通知されると、当該端末装置に対して当該ア
プリケーション記述ファイルを送信する過程と、

前記端末装置が、前記配信システムから送信されてくるアプリケーシ
ョン記述ファイルに内包されている前記セキュリティ記述ファイルの
15 格納位置を前記配信システムに通知する過程と、

前記配信システムが、前記通知されたセキュリティ記述ファイルの格
納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確
保された状態で前記端末装置に送信する過程と、

前記端末装置が、前記配信システムから送信された前記アプリケーシ
20 ョン記述ファイルに内包されている前記実体ファイルの格納位置を前
記配信システムに通知する過程と、

前記配信システムが、前記通知された実体ファイルの格納位置に基づ
いて、当該実体ファイルを前記端末装置に送信する過程と
を有する配信方法。

25 2. ネットワーク内の装置との通信を行うための通信部と、
記憶部と、
制御部とを具備し、
前記制御部は、

(a) アプリケーションを実現するためのソフトウェアを内包した実体ファイルの格納位置と、前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルの格納位置を示す情報を含んだ第1の配信要求を前記通信部により前記ネットワーク内の配信システムに送信することにより、前記配信システムにおける情報提供サーバ装置に格納されたアプリケーション記述ファイルを前記配信システムから前記通信部により受信し、前記記憶部に格納する手段と、

- 10 (b) 前記配信システムから受信されたアプリケーション記述ファイルに内包されている前記セキュリティ記述ファイルの格納位置を示す情報を含んだ第2の配信要求を前記通信部により前記配信システムに送信することにより、前記配信システムにおける管理サーバ装置に記憶されたセキュリティ記述ファイルを前記配信システムから前記通信部により受信し、前記記憶部に格納する手段と、

- 15 (c) 前記配信システムから受信されたアプリケーション記述ファイルに内包されている実体ファイルの格納位置を示す情報を含む第3の配信要求を前記通信部により前記配信システムに送信することにより、前記配信システムにおける情報提供サーバに格納された実体ファイルを前記配信システムから前記通信部により受信し、前記記憶部に格納する手段と、

- 20 (d) 前記記憶部に記憶された実体ファイルに含まれるソフトウェアの実行が指示された場合に、前記記憶部に記憶された該実体ファイルに対応したセキュリティ記述ファイルに含まれる権限情報に従い、該ソフトウェアの実行により実現されるアプリケーションの挙動を制限する手段と

を有する端末装置。

3. 前記配信システムは、前記セキュリティ記述ファイルを暗号化して

前記端末装置に送信することによってセキュリティを確保しており、

前記制御部は、前記配信システムによって送信されてくる暗号化されたセキュリティ記述ファイルを復号化する手段を具備する請求項 2 に記載の端末装置。

5

4. 前記制御部は、前記通信部により、セキュリティの確保された通信路を介して前記セキュリティ記述ファイルを受信する請求項 2 に記載の端末装置。

10

5. 前記制御部は、暗号化通信により前記セキュリティ記述ファイルを受信する請求項 2 に記載の端末装置。

15

6. 前記制御部は、前記通信部により、移動通信網および専用線を介して前記セキュリティ記述ファイルを受信する請求項 2 に記載の端末装置。

20

7. 前記制御部は、移動通信網を介した暗号化通信により前記セキュリティ記述ファイルを受信する請求項 2 に記載の端末装置。

8. 前記制御部におけるアプリケーションの挙動を制限する手段は、前記セキュリティ記述ファイルに内包された権限情報に基づき、資源の利用を制限する請求項 2 に記載の端末装置。

25

9. 前記資源は前記端末装置内部のハードウェア資源である請求項 8 に記載の端末装置。

10. 前記資源は前記端末装置外部の、当該端末装置が使用可能なハードウェア資源である請求項 8 に記載の端末装置。

1 1. 前記資源は前記端末装置内部のソフトウェア資源である請求項 8 に記載の端末装置。

1 2. 前記資源は前記端末装置外部の、当該端末装置が使用可能なソフトウェア資源である請求項 8 に記載の端末装置。

1 3. 前記資源は、前記端末装置が使用可能なネットワーク資源である請求項 8 に記載の端末装置。

10 1 4. 前記制御部におけるアプリケーションの挙動を制限する手段は、前記権限情報に基づき資源の利用の種類を判断する請求項 2 に記載の端末装置。

15 1 5. 前記アプリケーション記述ファイルは前記端末装置に通信サービスを提供する通信事業者の公開鍵を内包し、
前記セキュリティ記述ファイルは前記通信事業者の秘密鍵で署名されており、

20 前記制御部は、前記配信システムによって送信されてくるセキュリティ記述ファイルの正当性を前記アプリケーション記述ファイルに内包されている公開鍵を用いて検証し、その正当性が検証された場合にのみ、前記配信システムに対し前記実体ファイルの格納位置を通知する請求項 2 に記載の端末装置。

25 1 6. 前記アプリケーション記述ファイル及び前記セキュリティ記述ファイルは、対応するアプリケーションに割り当てられたアプリケーション識別子を内包しており、

前記制御部は、前記配信システムによって送信されてくるアプリケーション記述ファイルに内包されたアプリケーション識別子と、前記配信システムによって送信されてくるセキュリティ記述ファイルに内包さ

れたアプリケーション識別子とを比較し、両者が一致した場合にのみ、前記配信システムに前記実体ファイルの格納位置を通知する請求項 2 に記載の端末装置。

- 5 17. 前記アプリケーション記述ファイルに記述された前記セキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ、前記制御部は、前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する請求項 2 に記載の端末装置。
- 10 18. 前記セキュリティ記述ファイルは、対応するアプリケーションの有効期限を示す期限情報を内包しており、前記制御部は、前記配信システムに対して前記セキュリティ記述ファイルの格納位置を時系列的に繰り返し通知することによって、前記配信システムから当該セキュリティ記述ファイルが時系列的に繰り返し受信し、繰り返し受信される前記
- 15 セキュリティ記述ファイルに内包されている前記期限情報に基づいて、前記アプリケーションの有効期限を更新する手段を具備する請求項 2 に記載の端末装置。
- 20 19. 前記端末装置は、前記配信システムから前記セキュリティ記述ファイルが正当に配信されてきた場合にのみ、前記アプリケーションの有効期限を更新する請求項 18 に記載の端末装置。
- 25 20. 前記端末装置は移動機である請求項 2 に記載の端末装置。
- 26 21. アプリケーションを実現するためのソフトウェアを内包した実体ファイルと、前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルと、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述

されたアプリケーション記述ファイルを格納した1または複数のサーバ装置とを有し、

前記1または複数のサーバ装置のうち前記セキュリティ記述ファイルを格納するサーバ装置は、セキュリティ記述ファイルを管理する権限の

5 与えられた管理サーバ装置であり、

各々の前記サーバ装置は、ファイルの格納位置が通知されると当該ファイルをその通知元に返送する手段を有し、

前記管理サーバ装置は、前記セキュリティ記述ファイルの格納位置が通知されると当該セキュリティ記述ファイルをセキュリティが確保さ

10 れた状態で通知元に返送する

配信システム。

22. 通信部と、

記憶部と、

15 (a) ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを前記記憶部に書き込む処理と、

(b) 前記セキュリティ記述ファイルの有効性に関する情報を前記記憶部に書き込む処理と、

20 (c) 前記セキュリティ記述ファイルの有効性に関する問い合わせが前記通信部により端末装置から受信されたとき、当該セキュリティ記述ファイルの有効性に関する情報を前記記憶部から読み出し、前記通信部により前記端末装置に通知する処理と

を行う制御部とを具備する管理サーバ装置。

25

23. 通信部と、

記憶部と、

(a) ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイ

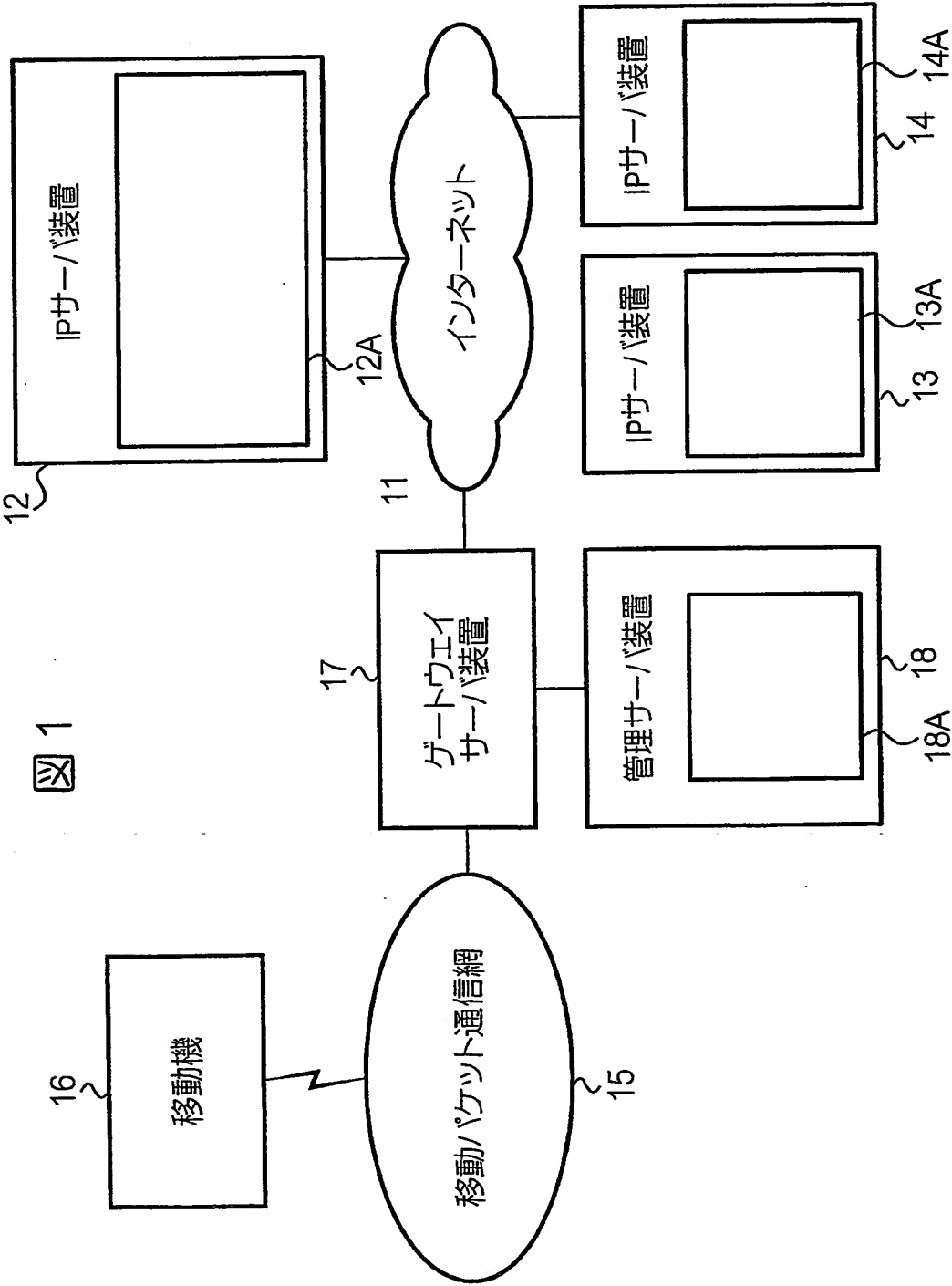
ルを前記通信部により管理サーバから受信し、前記記憶手段に書き込む処理と、

(b) 前記記憶手段に格納されたセキュリティ記述ファイルの有効性に関する問い合わせを前記通信部により前記管理サーバ装置に繰り返し

5 送信する処理と、

(c) 前記セキュリティ記述ファイルが失効している旨の回答が前記通信部により前記管理サーバ装置から受信された場合に、当該セキュリティ記述ファイルに対応付けられた実体ファイルを起動不能状態にする処理と

10 を実行する制御部とを具備する端末装置。



2/18

図 2

APID	ハッシュ値	パッケージURL	...	SDF-URL	公開鍵
------	-------	----------	-----	---------	-----

図 3

APID	ポリシー情報	有効期限
------	--------	------

図 4

トラステッドAPI	パーミッション
getPhoneList()	○
getCallHistory()	×
getMsStatus()	○

3/18

図 5

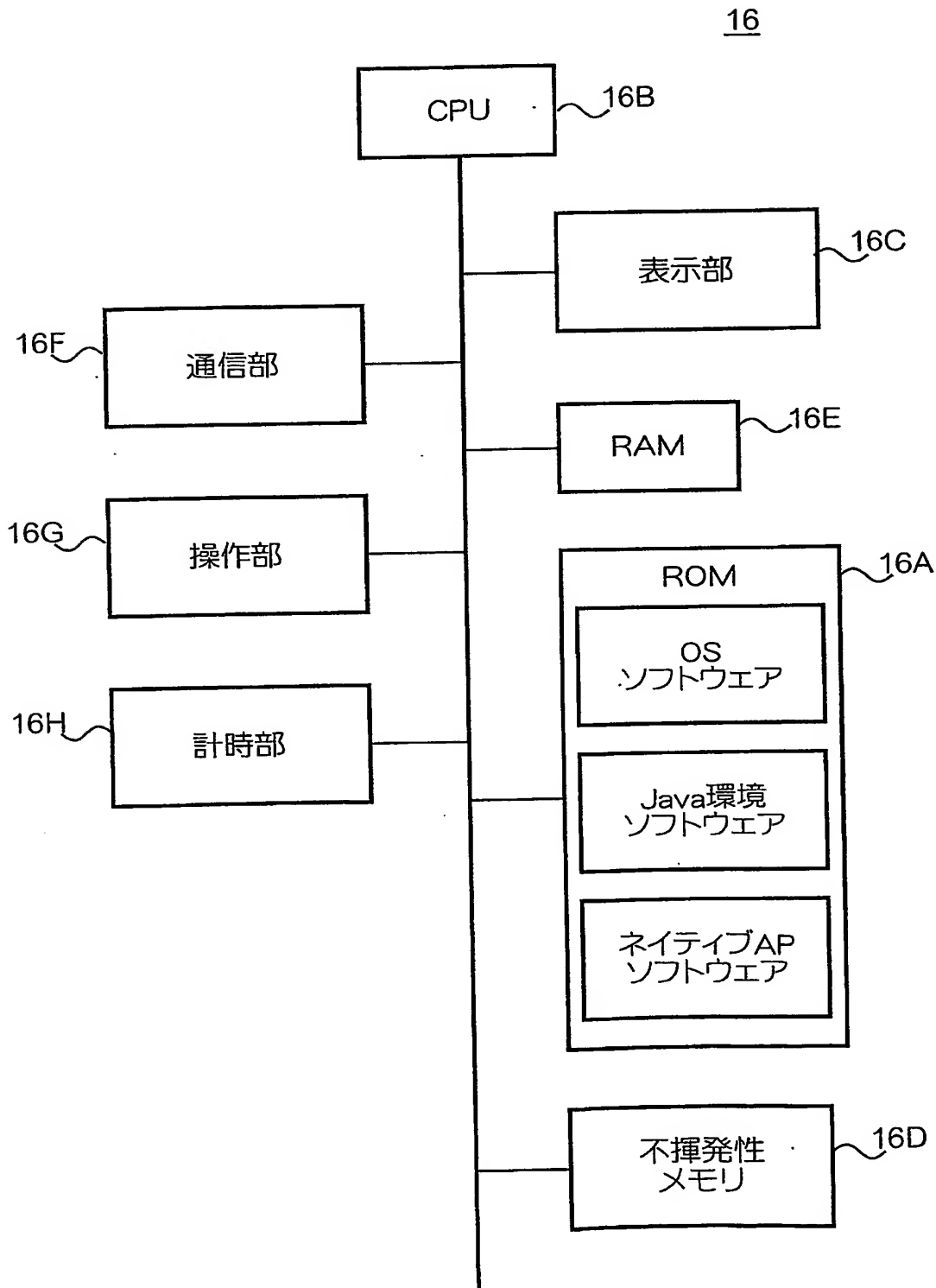


図 6

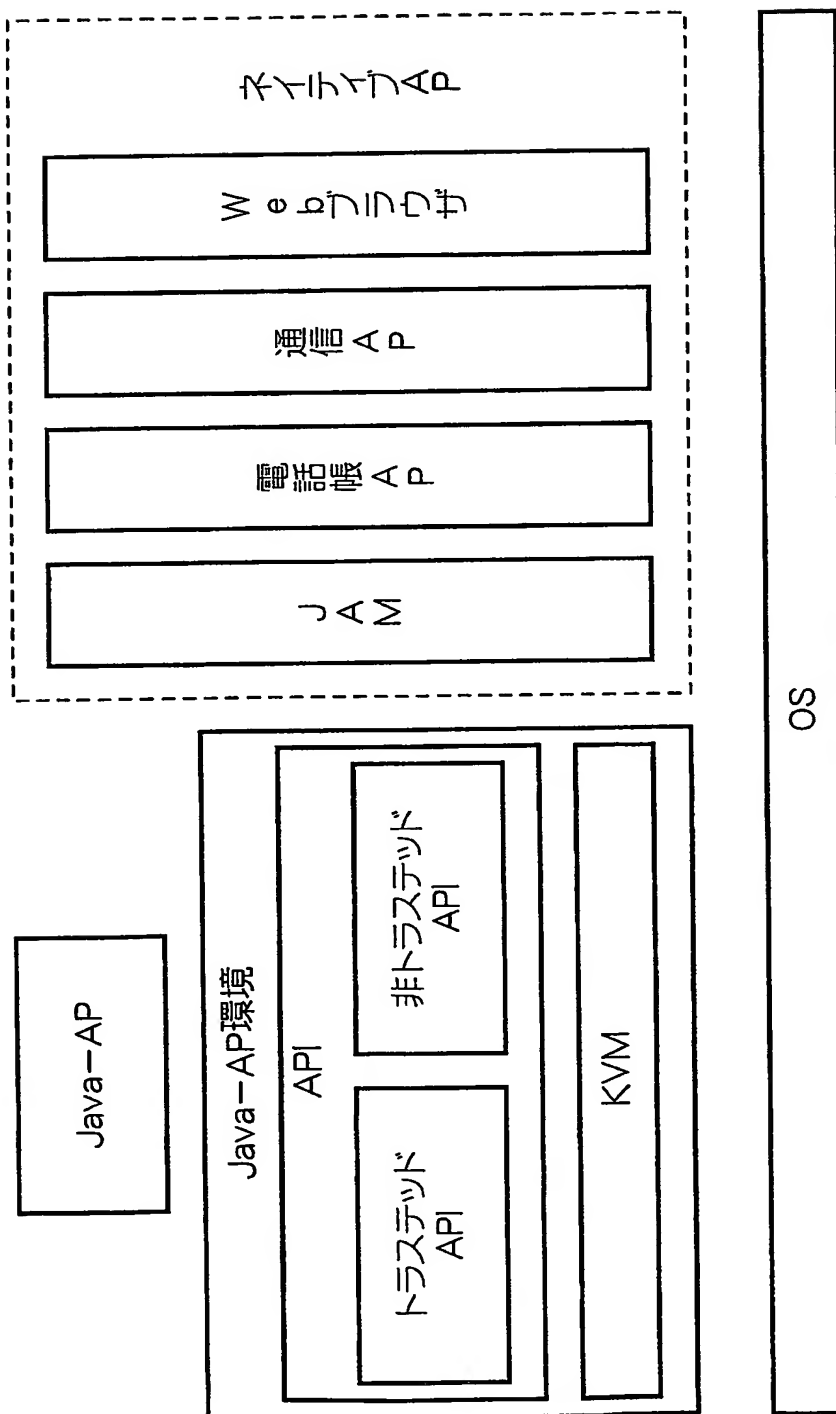


図 7

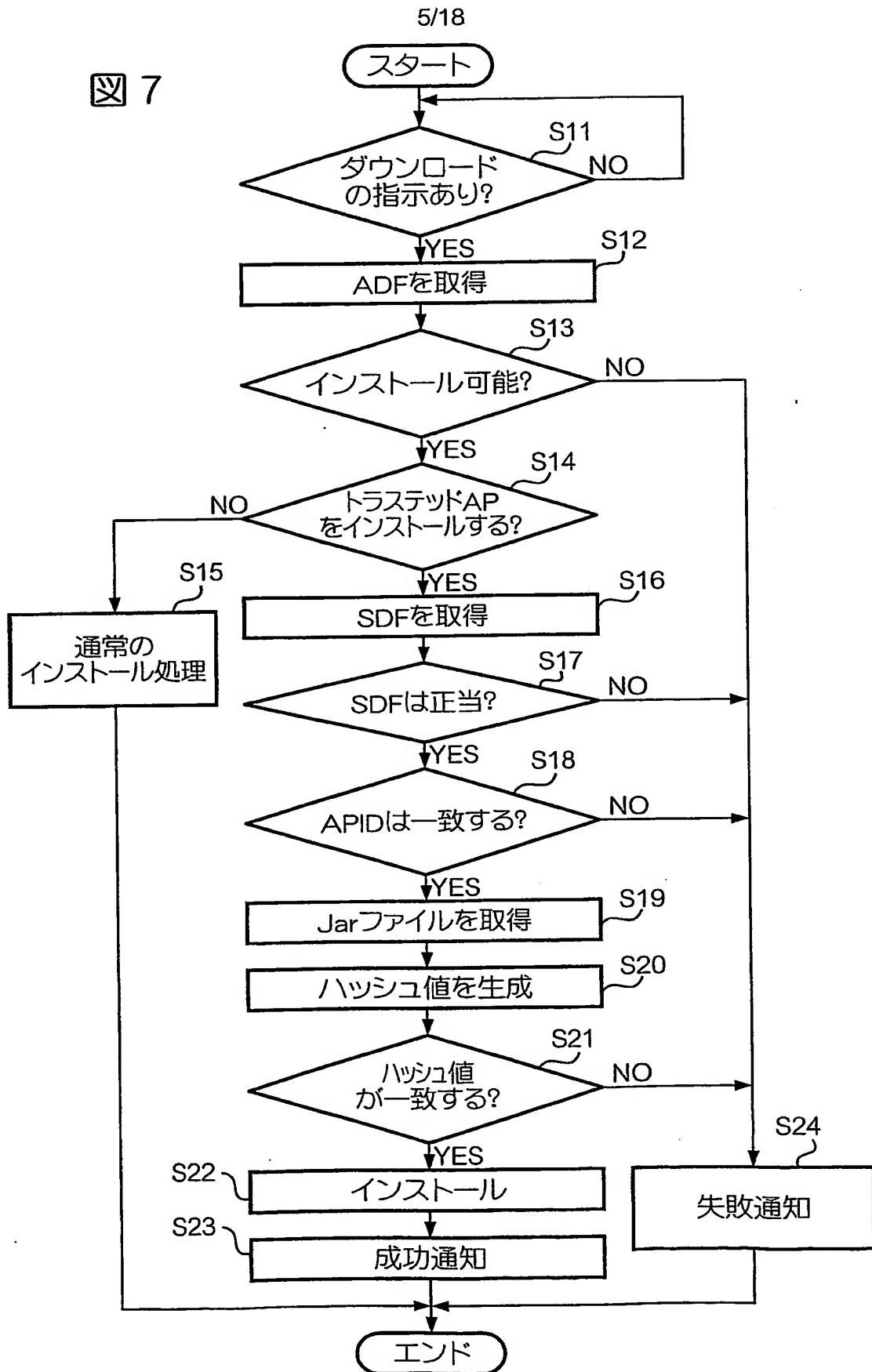
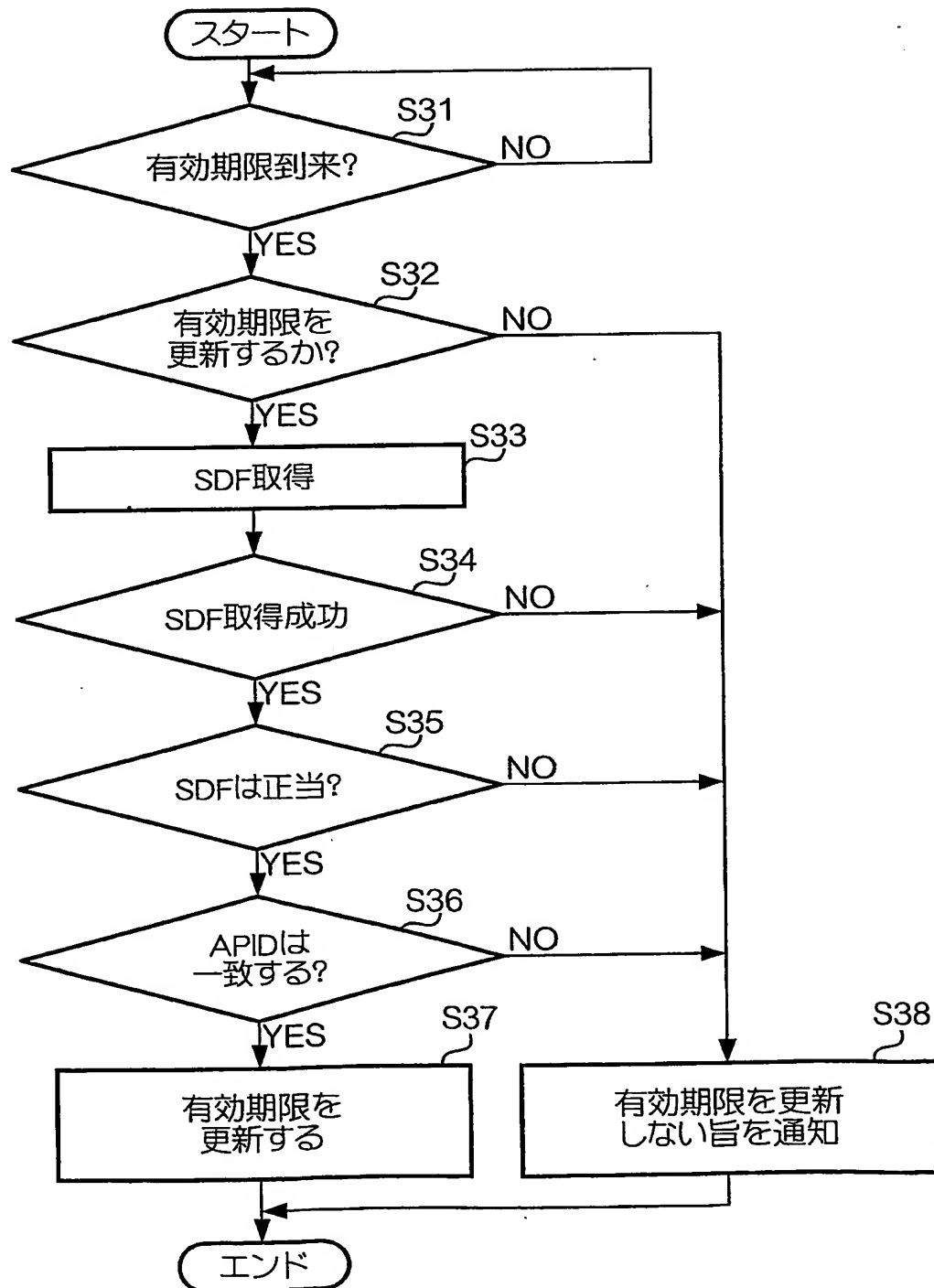


図 8



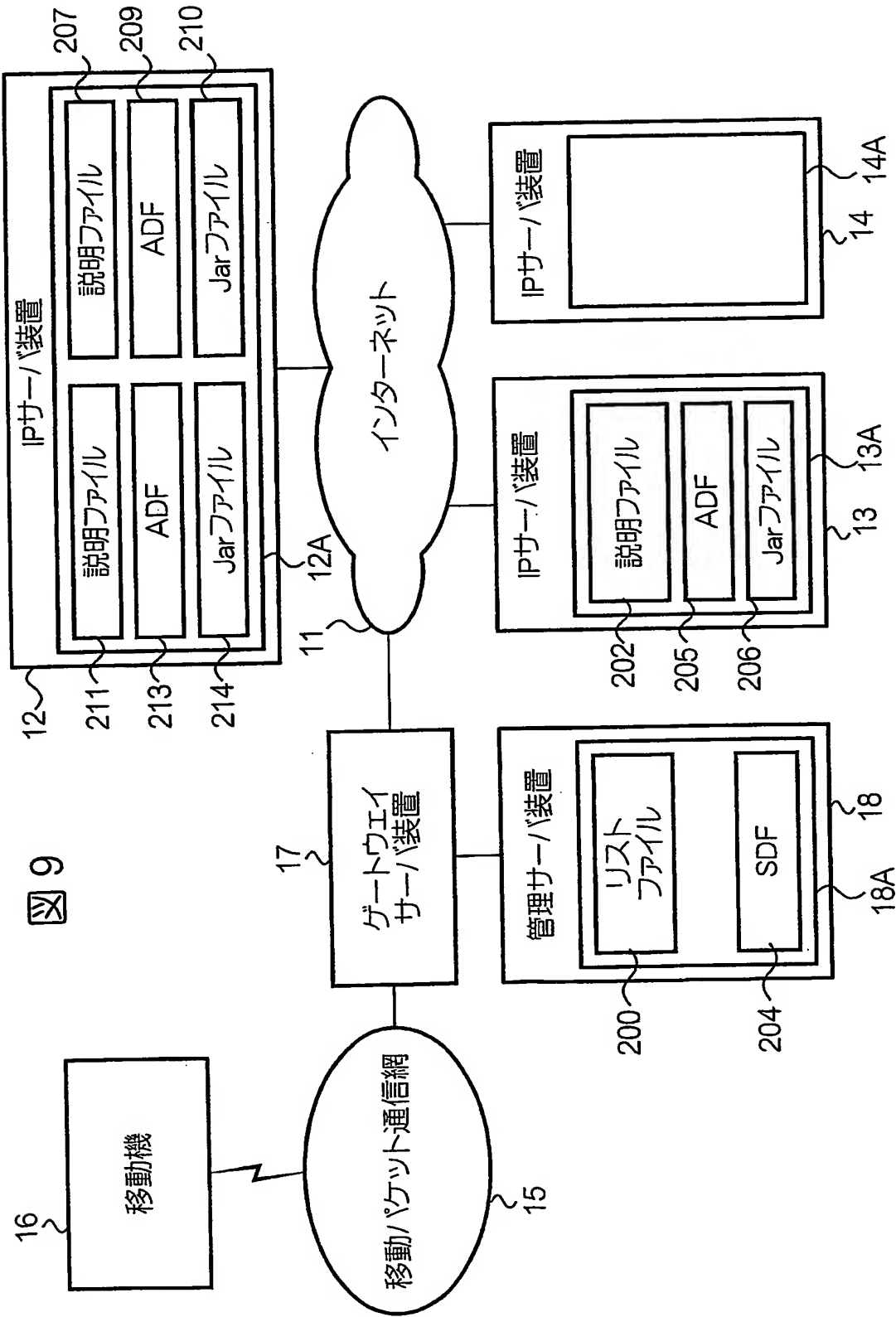


図 10

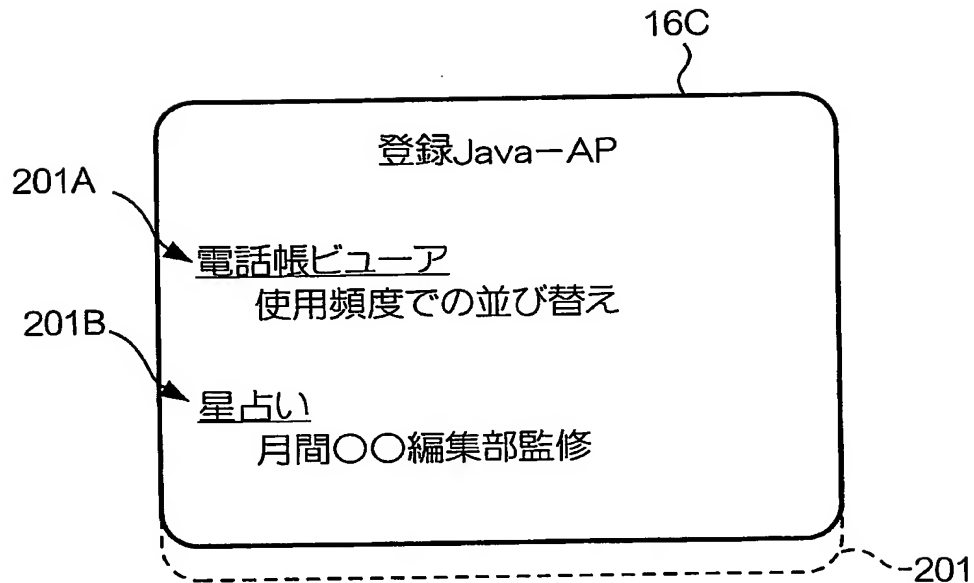


図 11

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/shogi.jam">
詰め将棋
</OBJECT>
  ~するソフトウェアです。ダウンロードするには
  <A ijam="#application.declaration">ここ</A>
をクリック。
```

9/18

図 12

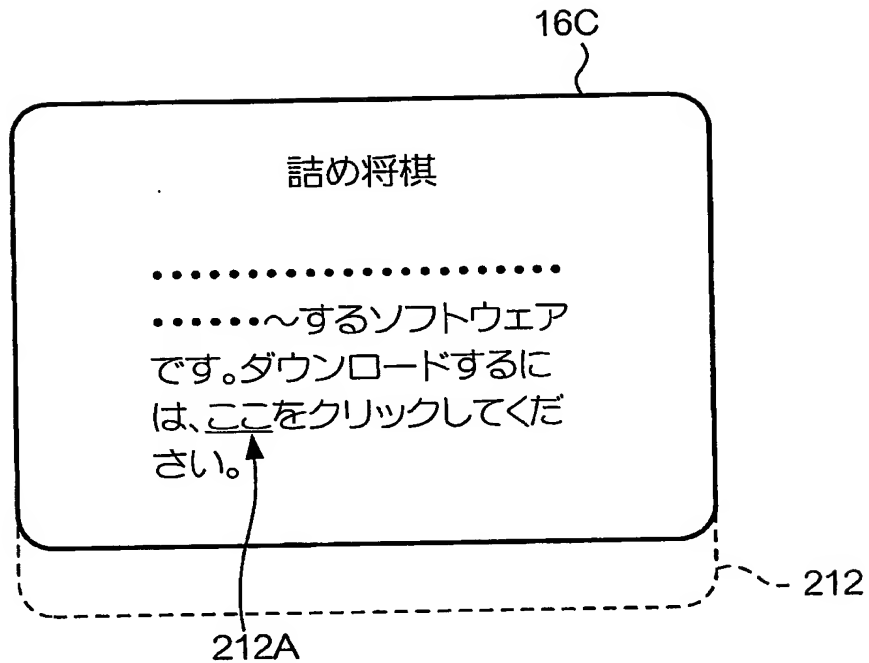


図 13

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/horoscope.jam">
星占い
</OBJECT>
  ~するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。
```

10/18

図 14

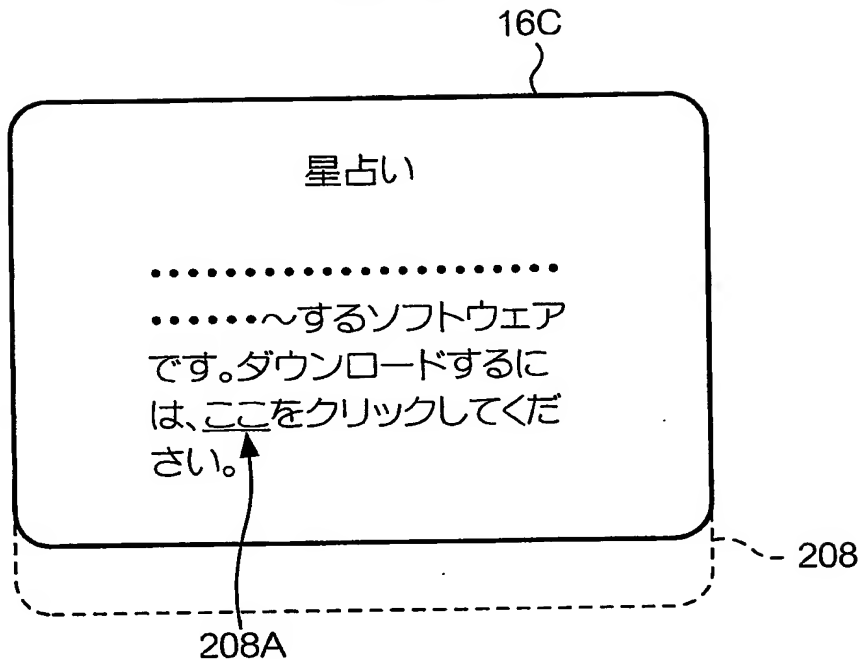


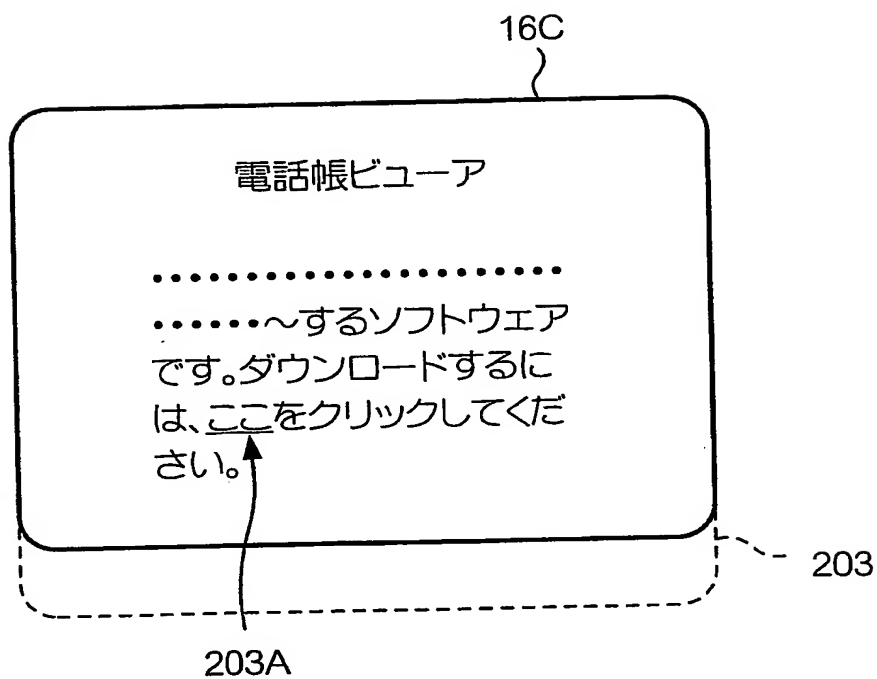
図 15

```

<OBJECT declare id="application.declaration"
data="http://www.aaa.co.jp/viewer.sdf"
type="application/x-jam">
  電話帳ビューア
</OBJECT>
  ~するソフトウェアです。ダウンロードするには
  <A ijam="#application.declaration">ここ</A>
  をクリック。

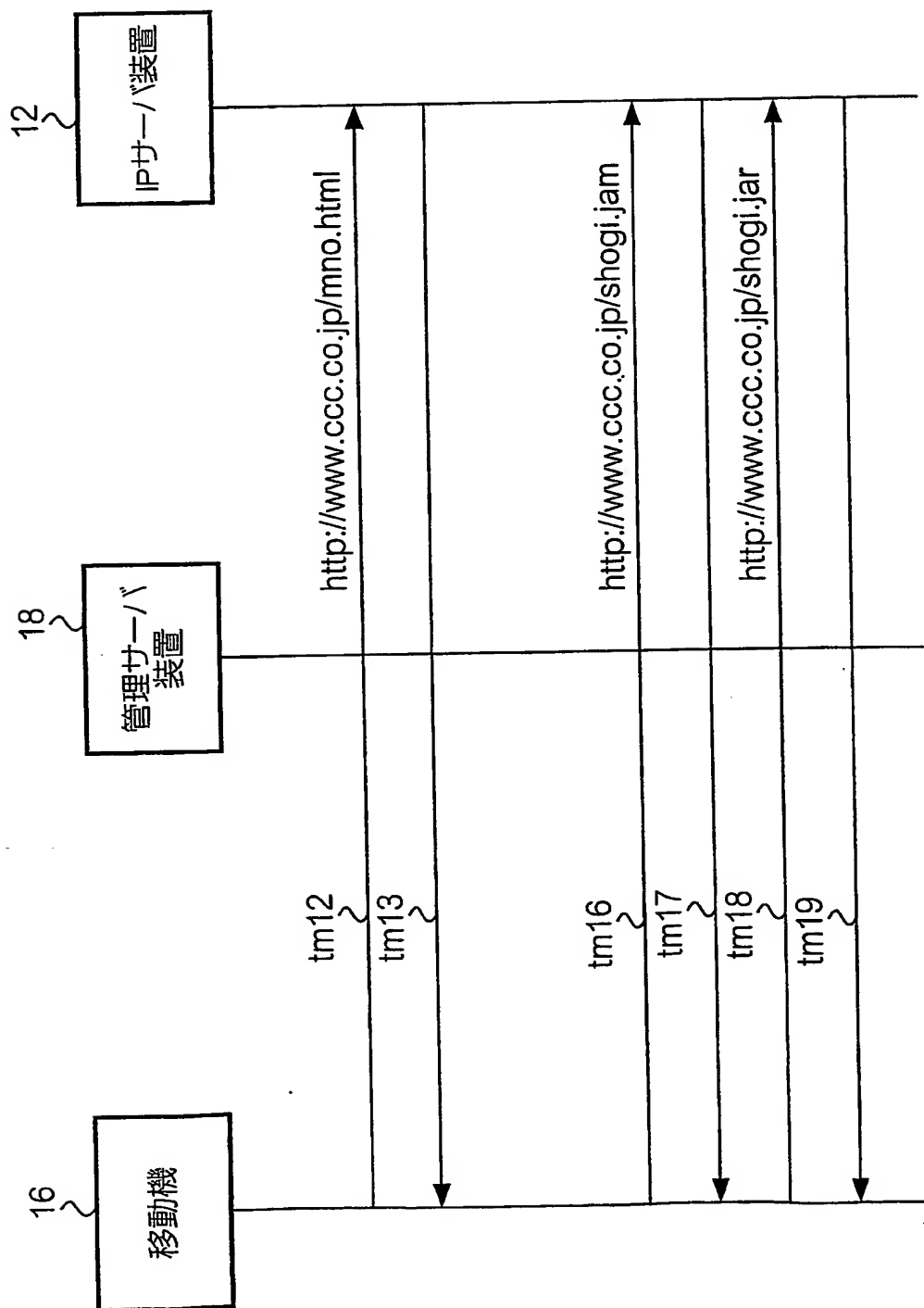
```

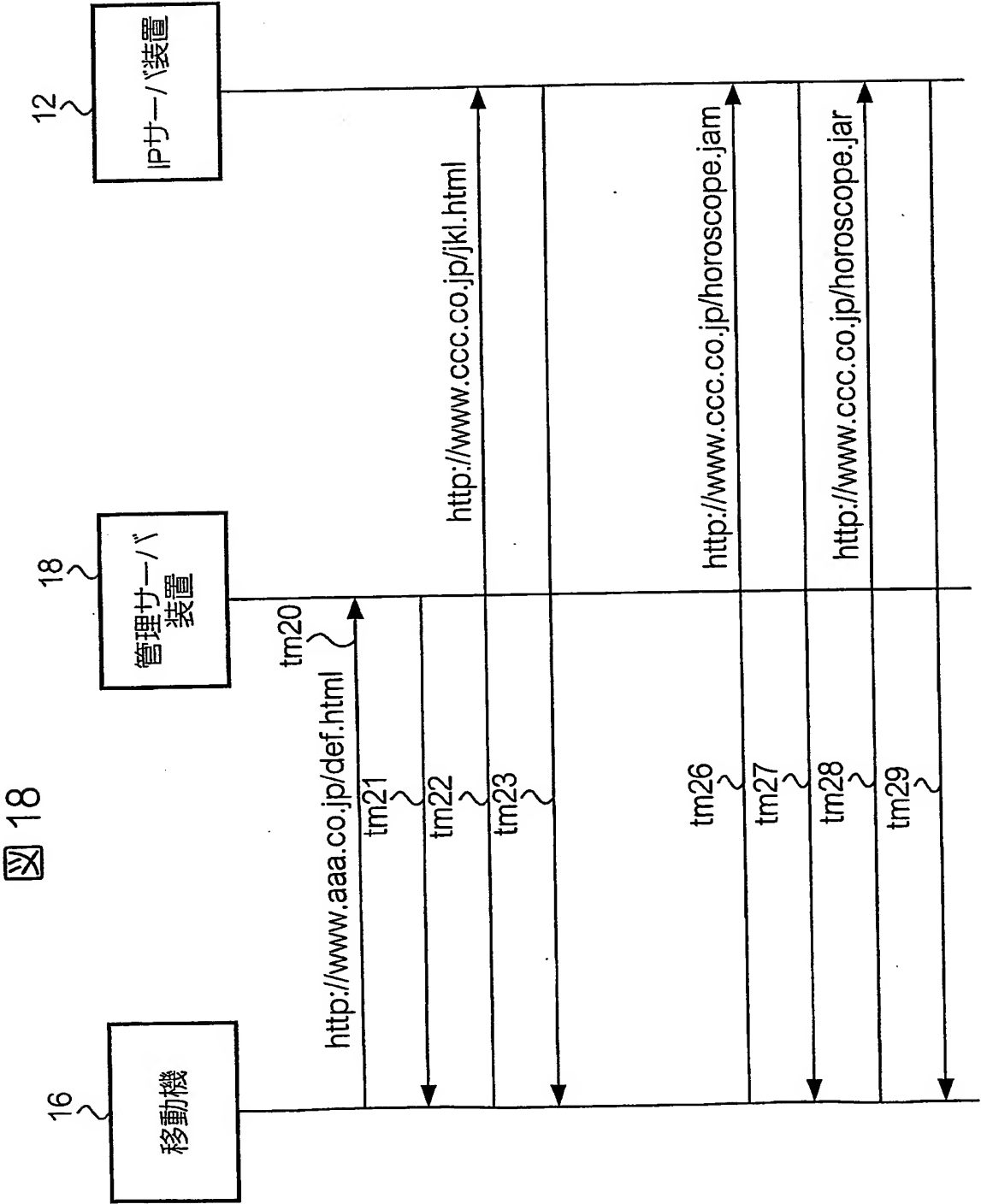
図 16

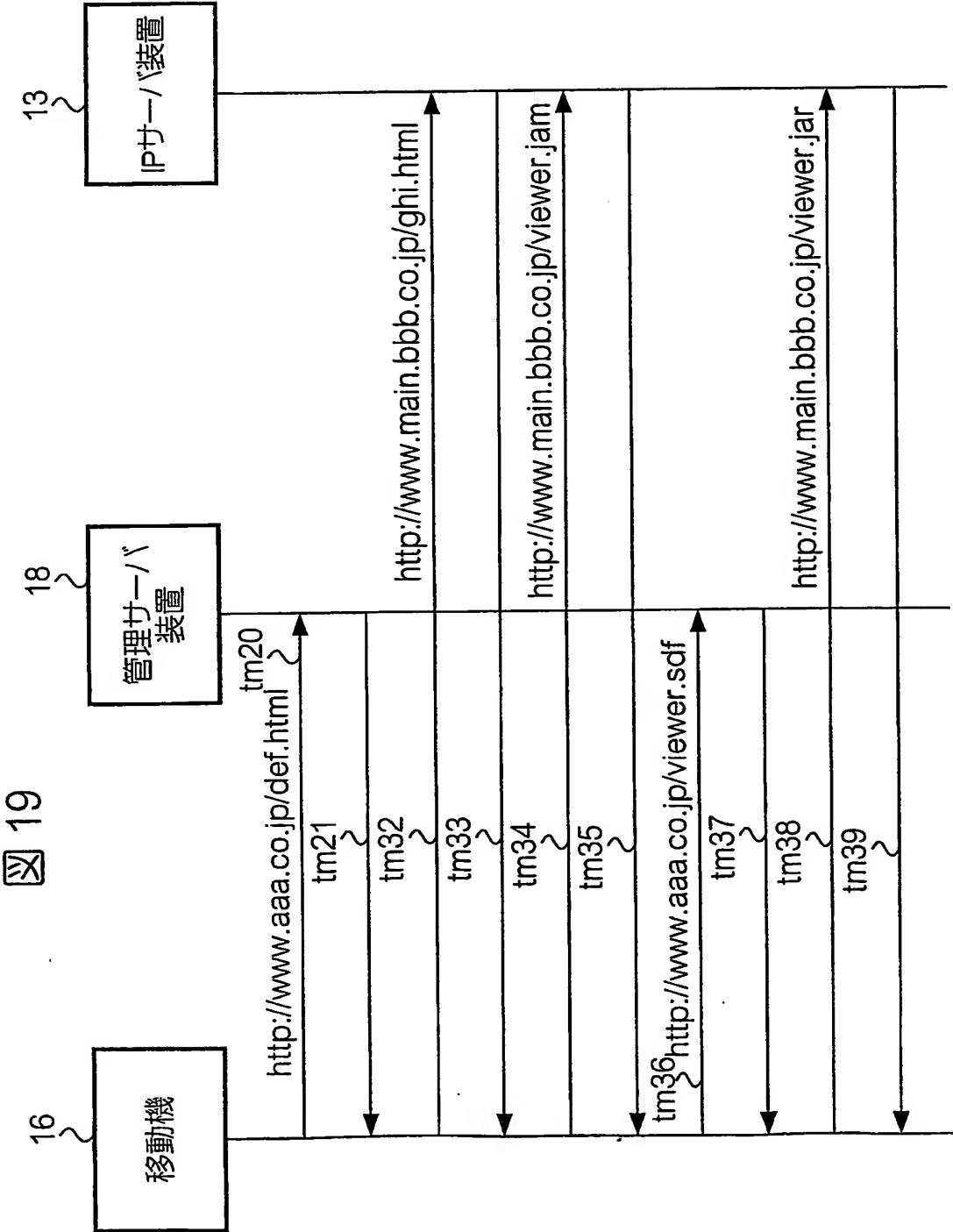


12/18

図 17







15/18

図 20

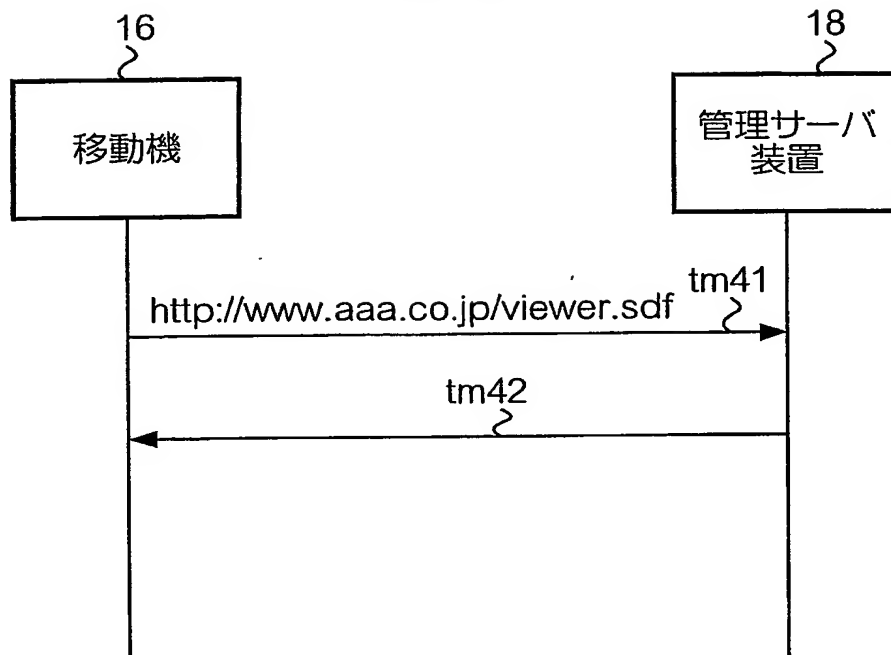
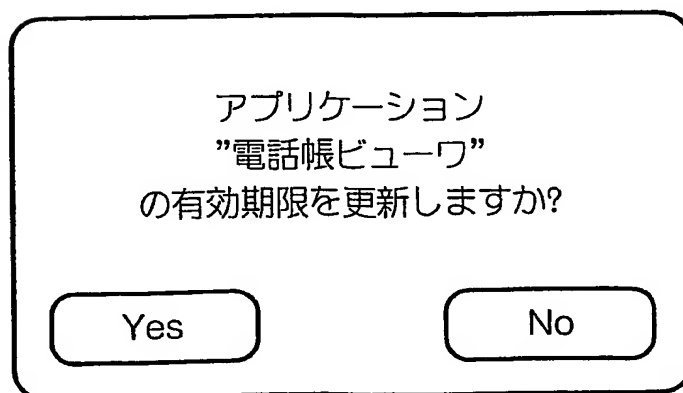


図 21



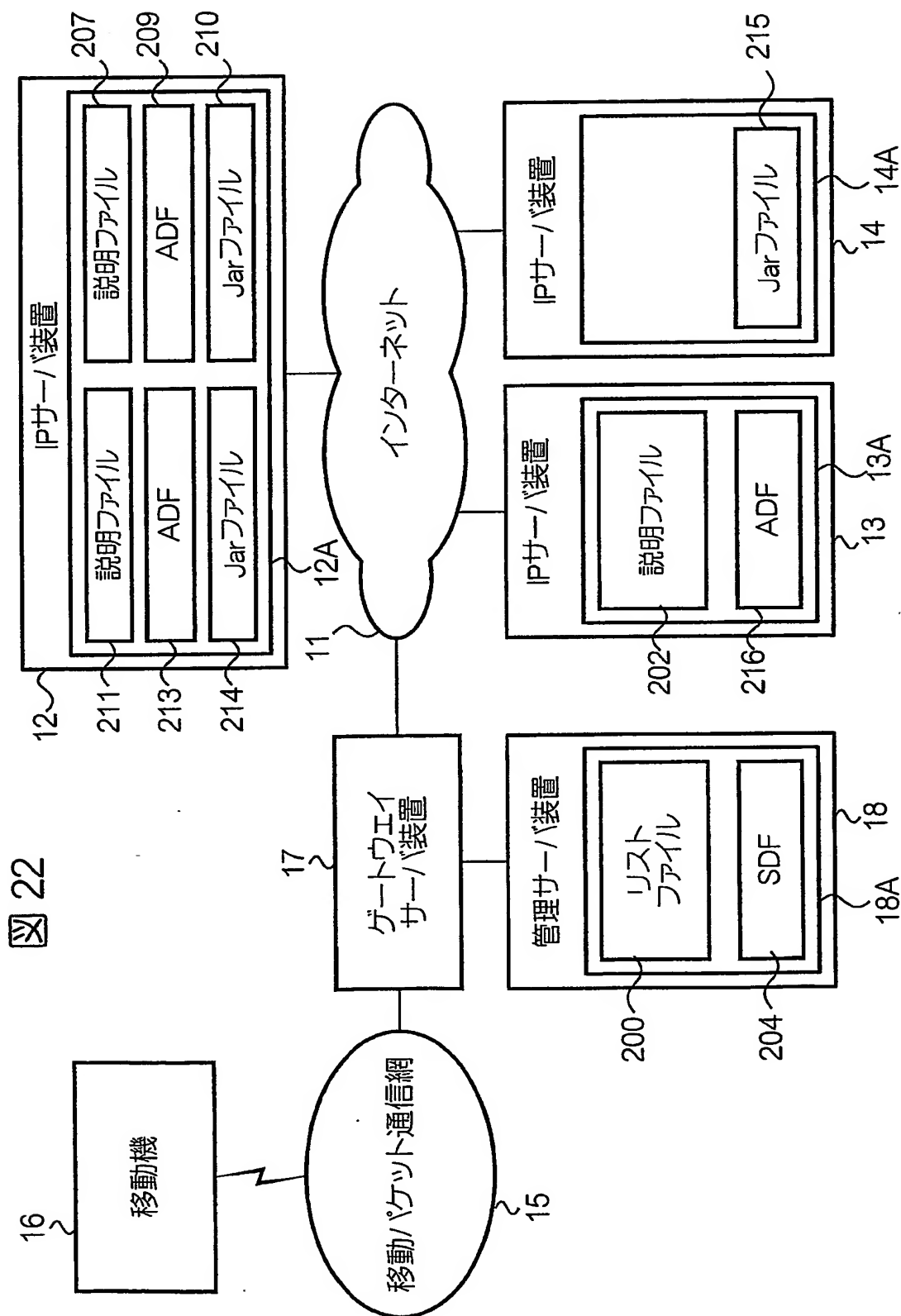
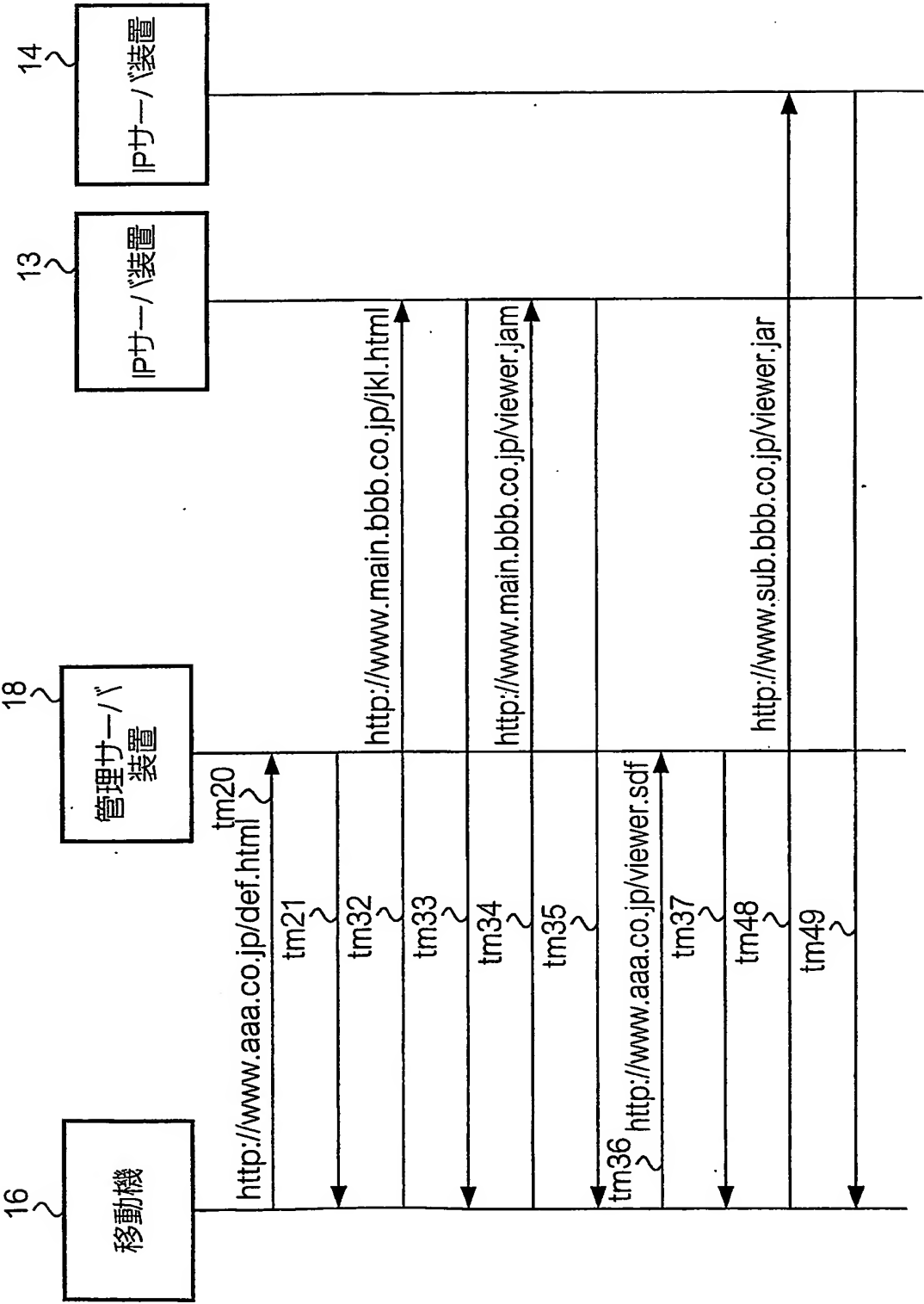
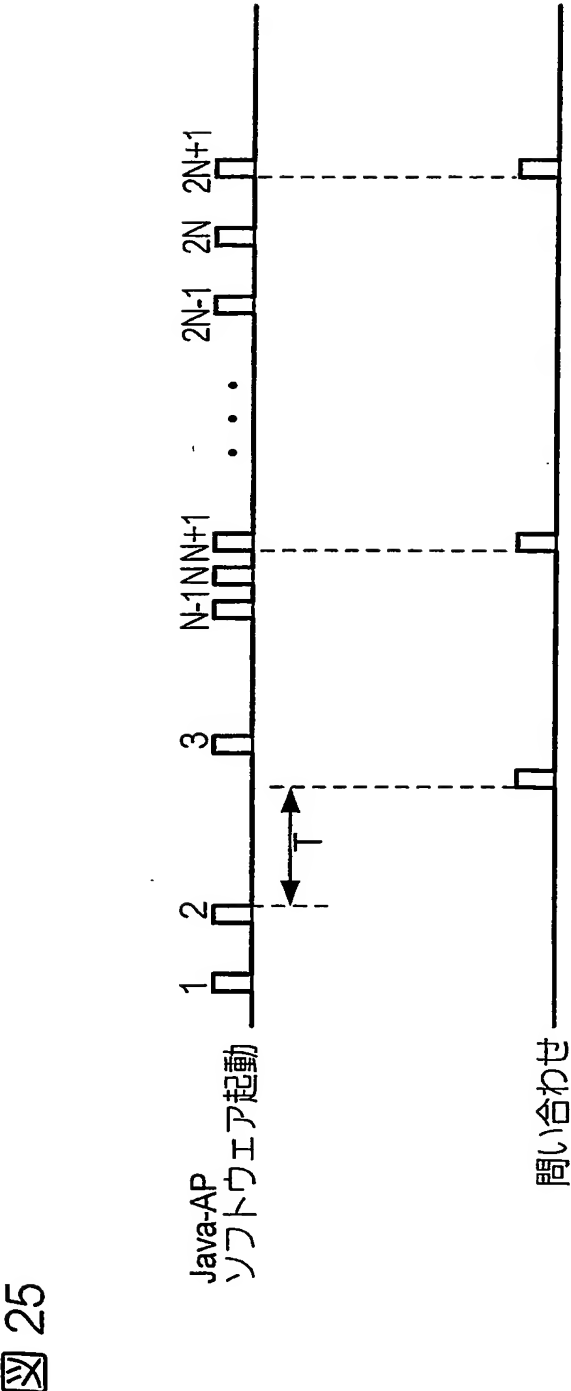
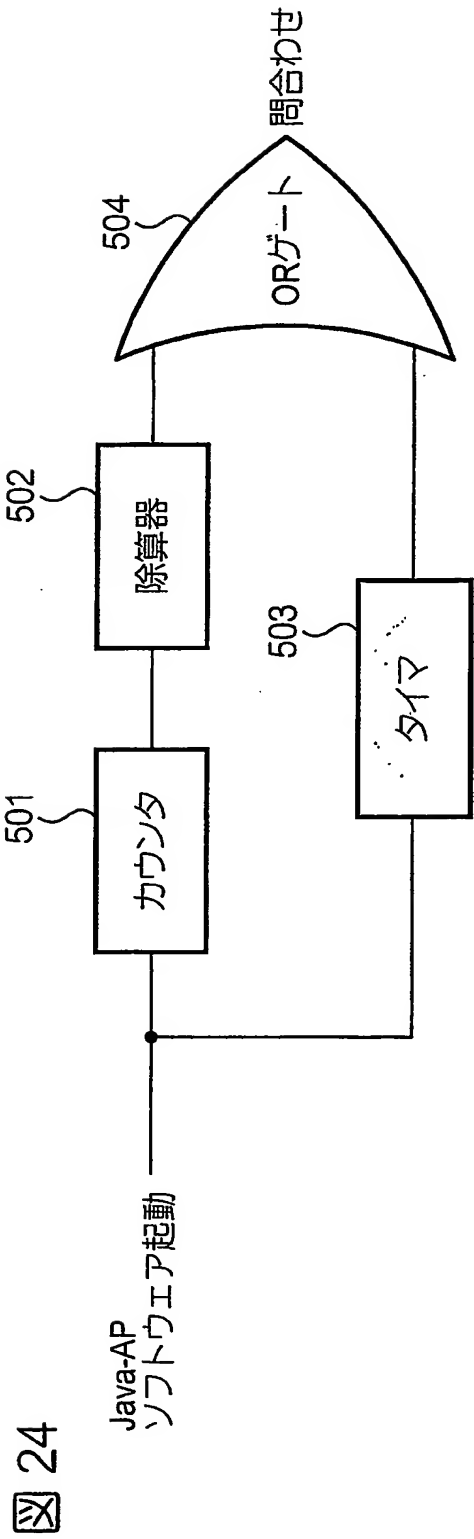


図 23





INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/03974

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F9/06, G06F13/00, H04M11/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F9/06, G06F13/00, H04M11/00, G06F12/14, G06F15/00,
G06F15/16, G06F9/44-9/46

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE(JOIS) in Japanese
Computer Software DataBase(Japanese Patent Office) in Japanese
INSPEC(DIALOG) in English

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	Edited by ASCII Shoseki Henshubu "i-Mode Java programming - Stand Alone Application Part revised new edition", first edition, Ascii Corp., 21 May, 2001 (21.05.01), ISBN: 4-7561-3790-3, pages 40 to 52(particularly, page 47, table 3-2; page 47, lines 5 to 9; page 48, last line to page 49, line 2)	1-14,16-23 15
Y A	Li Gong, "Java Series Java2 Platform Security", first edition, Kabushiki Kaisha Pearson Education, 30 November, 2000 (30.11.00), ISBN: 4-89471-193-1, pages 123 to 125, 134 to 138 (particularly, page 123, lines 18 to 22; page 124, lines 20 to 22; page 125, section 4.2.2)	1-14,16-23 15

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
10 June, 2003 (10.06.03)

Date of mailing of the international search report
24 June, 2003 (24.06.03)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/03974

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	Computer Today, 01 September, 1998 (01.09.98), Vol.15, No.5, pages 44 to 49, ISBN: 0289-3509 (particularly, page 47, left column, lines 28 to 29, "File Permission", "Socket Permission", "Net Permission")	1-14, 16-23 15
A	EP 0813132 A2 (International Business Machines Corp.), 17 December, 1997 (17.12.97), Page 2, lines 20 to 21; page 3, lines 45 to 48 & US 5825877 A & JP 10-083310 A	1-23

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F9/06, G06F13/00, H04M11/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F9/06, G06F13/00, H04M11/00, G06F12/14,
G06F15/00, G06F15/16, G06F9/44-9/46

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2003年
 日本国登録実用新案公報 1994-2003年
 日本国実用新案登録公報 1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JSTファイル (JOIS) 日本語,
 ComputerSoftwareDataBase (日本国特許庁) 日本語,
 INSPEC (DIALOG) 英語

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	アスキー書籍編集部・編、「iモードJavaプログラミングース タンドアロン・アプリケーション編 改訂新版」、初版、株式会社 アスキー、2001.05.21、ISBN: 4-7561-37 90-3、pp. 40~52 (特に第47頁の表3-2、第47頁 第5~9行、第48頁末行~第49頁第2行)	1-14, 16-23
A		15

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

10.06.03

国際調査報告の発送日

24.06.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

久保 光宏

5B 9189

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	Li Gong, 「Java Series Java 2 プラット フォームセキュリティ」、初版、株式会社ピアソン・エデュケー ション、2000. 11. 30、ISBN: 4-89471-193 -1、pp. 123~125 及び 134~138 (特に第123頁	1-14, 16-23
A	第18~22行、第124頁第20~22行、第125頁の 4. 2. 2節)	15
Y	Computer Today, 1998. 09. 01, Vol. 15, No. 5, pp. 44~49, ISSN: 0289 -3509 (特に第47頁左コラム第28~29行の" File P ermission"、" Socket Permission"、	1-14, 16-23
A	" Net Permission" という記載)	15
A	EP 0813132 A2 (International Business Machines Corporation). 1997. 12. 17, 第2頁第20~21行、第3頁第45~4 8行, & US 5825877 A, & JP 10-083310 A	1-23